(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2001年6月7日 (07.06.2001)

PCT

(10) 国際公開番号
WO 01/41359 A1

(51) 国際特許分類[7]: H04L 9/32, G06F 12/14, G10K 15/02, G06F 13/00

(21) 国際出願番号: PCT/JP00/08497

(22) 国際出願日: 2000年12月1日 (01.12.2000)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願平11/345244 1999年12月3日 (03.12.1999) JP

(71) 出願人 (米国を除く全ての指定国について): 三洋電機株式会社 (SANYO ELECTRIC CO., LTD.) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 Osaka (JP). 株式会社 ピーエフユー (PFU LIMITED) [JP/JP]; 〒929-1125 石川県河北郡宇ノ気町字宇野気ヌ98番地の2 Ishikawa (JP). 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 Kanagawa (JP). 株式会社 日立製作所 (HITACHI, LTD.) [JP/JP]; 〒101-8010 東京都千代田区神田駿河台四丁目6番地 Tokyo (JP). 日本コロムビア株式会社 (NIPPON COLUMBIA CO., LTD.) [JP/JP]; 〒107-8011 東京都港区赤坂四丁目14番14号 Tokyo (JP).

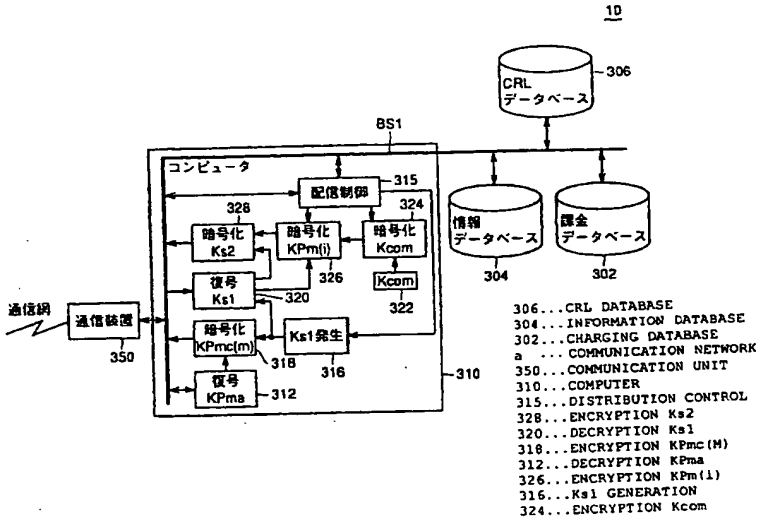
(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 堀 吉宏 (HORI, Yoshihiro) [JP/JP]. 日置敏昭 (HIOKI, Toshiaki) [JP/JP]. 金森美和 (KANAMORI, Miwa) [JP/JP]. 吉川隆敏 (YOSHIKAWA, Takatoshi) [JP/JP]. 武村浩司 (TAKEMURA, Hiroshi) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内 Osaka (JP). 高橋政孝 (TAKAHASHI, Masataka) [JP/JP]; 〒929-1125 石川県河北郡宇ノ気町字宇野気ヌ98番地の2 株式会社 ピーエフユー内 Ishikawa (JP). 長谷部高行 (HASEBE, Takayuki) [JP/JP]. 古田茂樹 (FURUTA, Shigeki) [JP/JP]. 畠山卓久 (HATAKEYAMA, Takahisa)

[続葉有]

(54) Title: DATA DISTRIBUTION SYSTEM AND RECORDER FOR USE THEREIN

(54) 発明の名称: データ配信システムおよびそれに用いられる記録装置



(57) Abstract: A license server (10) comprises a CRL database (306) for holding a prohibition list containing a specified class for which distribution, reproduction, and transfer of content data are prohibited among predetermined classes corresponding to a storage device, e.g. a memory card, and a content reproducing circuit, e.g. a portable telephone. A distribution control section (315) stops distribution if the destination class is contained in the prohibition list when the content data is distributed. The prohibition list is also held in the memory card, and the distribution control section (315) also transmits information for updating the prohibition list in the memory card when the content is distributed.

[続葉有]

WO 01/41359 A1

[JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP). 利根川忠明 (TONEGAWA, Tadaaki) [JP/JP]; 〒187-8588 東京都小平市上水本町五丁目20番1号 株式会社 日立製作所 半導体グループ内 Tokyo (JP). 穴澤健明 (ANAZAWA, Takeaki) [JP/JP]; 〒107-8011 東京都港区赤坂四丁目14番14号 日本コロムビア株式会社内 Tokyo (JP).

(74) 代理人: 深見久郎, 外(FUKAMI, Hisao et al.) ; 〒530-0054 大阪府大阪市北区南森町2丁目1番29号 住友銀行南森町ビル Osaka (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

ライセンスサーバ（１０）は、記憶装置たとえばメモリカードである記憶装置および、たとえば形態電話機であるコンテンツ再生回路にそれぞれ対応して予め定められるクラスのうちの、コンテンツデータの配信、再生および移動の禁止対象とされる特定のクラスを記録する禁止リストを保持するＣＲＬデータベース（３０６）を備える。配信制御部（３１５）は、コンテンツデータの配信時において、配信先のクラスが禁止リストに含まれる場合は配信動作を中止する。禁止リストは、メモリカード内にも保持され、配信制御部（３１５）は、コンテンツ配信時において、メモリカード内の禁止リストを更新するための情報を併せて送信する。

明細書

データ配信システムおよびそれに用いられる記録装置

技術分野

本発明は、携帯電話機等の端末に対して情報を配送するためのデータ配信システムに関し、さらに詳しくは、コピーされた情報に対する著作権保護を可能とするデータ配信システムおよび当該システムで用いられメモリカードに関する。

背景技術

近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

したがって、このような情報通信網上において音楽データや画像データ等の著作者の権利が存在するコンテンツデータが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介してコンテンツデータの配信を行なうことができないとすると、基本的には、コンテンツデータの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したＣＤ（コンパクトディスク）については、ＣＤから光磁気ディスク（ＭＤ等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に

止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

しかも、CDからMDへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化のほとんどないデジタルデータであることに鑑み、記録可能なMDからさらに他のMDにコピーすることは、著作権保護のために機器の構成上できないようになっている。

このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

この場合、情報通信網を通じて公衆に送信されるコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

発明の開示

この発明の目的は、情報通信網、たとえば携帯電話機等の情報通信網を介してコンテンツデータを配信することが可能なデータ配信システムおよび当該データ配信システムで使用される記録装置、詳しくはメモリカードを提供することである。

この発明の他の目的は、配信されたコンテンツデータが、著作権者の許可なく複製されることを防止することが可能なデータ配信システムおよび当該データ配信システムで使用される記録装置、詳しくはメモリカードを提供することである。

この発明に従うと、データ配信システムは、複数の端末と、コンテンツ供給装置とを備える。各端末は、外部との間でデータを授受するための第１のインタフェース部と、少なくともライセンスキーを受けて記録する配信データ解読部とを含む。配信データ解読部は、認証鍵によって復号することで認証可能な状態に暗号化された、配信データ解読部に対応して定められる第１のクラス証明データを保持し、ライセンスキーを受信する場合に、第１のインタフェース部を介して出力する第１の認証データ保持部と、暗号化コンテンツデータおよびライセンスキ

一を記録するための第１の記憶部とを有する。コンテンツ供給装置は、外部との間でデータを授受するための第２のインタフェース部と、認証鍵によって復号することで正当性を証明できる状態に暗号化された第１のクラス証明データを第２のインタフェース部から受け取って、認証鍵によって復号して正当性を確認するための第１の認証処理部と、配信の禁止対象となされる第１のクラス証明データをリストアップした禁止クラスリストを保持するための禁止クラスリスト保持部と、第１の認証処理部において得られた第１のクラス証明データが禁止クラスリスト保持部に保持される禁止クラスリストに含まれる場合には、少なくともコンテンツキーの配信動作を中止する配信制御部とを含む。

好ましくは、各端末は、コンテンツ再生部をさらに含む。コンテンツ再生部は、配信データ解読部からライセンスキーと暗号化コンテンツデータとを受けて、ライセンスキーにより暗号化コンテンツデータを復号して再生するコンテンツデータ再生部と、認証鍵によって復号することで正当性が証明できる状態に暗号化された、コンテンツ再生部に対応して予め定められる、第２のクラス証明データを保持する第２の認証データ保持部とを有し、第１の認証処理部は、暗号化された第２のクラス証明データを、第２のインタフェース部から受け取って復号処理を行なう。禁止クラスリスト保持部に保持された禁止クラスリストは、禁止対象とされる第２のクラス証明データをさらにリストアップする。配信動作において、各端末は、暗号化された第２のクラス証明データを第１のインタフェース部を介して第２のインタフェース部に対して出力する。配信制御部は、第２のインタフェース部を介して入力され、第１の認証処理部によって復号された第２のクラス証明書データが、禁止クラスリスト保持部に保持される禁止クラスリストに含まれる場合には、配信動作を中止する。

このような、データ配信システムにおいては、配信動作において、配信データ解読部（メモリカード）およびコンテンツ再生部（携帯電話機）の少なくとも一方のクラスを確認して、クラスごとに配信動作を禁止することが可能である。したがって、たとえば、固有鍵が破られたクラスに対しては、配信動作を実行できないようにすることができる。この結果、正規の著作権を保護できる記録装置や再生装置を持つユーザのみがコンテンツデータを受信してメモリカード中に格納

し、復号して利用することが可能となり、かつ無制限なコピーによって著作権者が不当な不利益を被ることを防止することが可能となる。

この発明の別の局面に従うと、記録装置は、第１の記憶部と、認証処理部と、第２の記憶部と、制御部とを備える。第１の記憶部は、データを記録する。認証処理部は、インタフェース部を介して入力される、認証鍵によって復号することで認証可能な状態に暗号化された第１のクラス証明データを受けて、認証鍵による復号を行なって正当性を確認する。第２の記憶部は、データの出力を禁止する対象となされる第１のクラス証明データをリストアップした禁止クラスリスト（CRL）を保持する。制御部は、外部からのデータの出力指示に応じて、インタフェース部を介してデータの出力を指示する。制御部は、出力指示とともに外部からインタフェース部を介して入力される、暗号化がなされた第１のクラス証明データを認証処理部で復号して得られる第１のクラス証明データが禁止クラスリストに含まれる場合には、データの出力を中止する。

好ましくは、記録装置は、認証鍵によって復号可能な状態に暗号化された、記録装置に対応して定められる第２のクラス証明データを保持する認証データ保持部をさらに備える。認証データ保持部は、外部からのデータの入力指示に応じて、認証データ保持部に保持される、認証鍵によって復号することで正当性を証明できる状態に暗号化された第２のクラス証明データをインタフェース部を介して出力する、

このような、記録装置においては、ライセンスキー等のデータの入出力時において、データの出力先あるいは記録装置自身のクラスを確認して、クラスごとに入出力動作の実行を禁止することが可能である。したがって、たとえば、固有鍵が破られたクラスに対しては、データの入出力を実行できないようにすることができる。この結果、正規の著作権を保護できる記録装置や再生装置を持つ正規のユーザのみがデータを受信して記録装置中に格納し、復号して利用することが可能となり、かつ無制限なコピーによって著作権者が不当な不利益を被ることを防止することが可能となる。

図面の簡単な説明

図１は、本発明のデータ配信システムの全体構成を概略的に説明するための概念図である。

図２は、実施の形態１に従うデータ配信システムにおいて使用される通信のためのデータ、情報等の特性を説明する図である。

図３は、実施の形態１に従うデータ配信システムにおいて使用される認証および禁止クラスリストの運用のためのデータ、情報等の特性を説明する図である。

図４は、実施の形態１に従うデータ配信システムにおいて暗号化に関わる鍵の特性をまとめて説明する図である。

図５は、図１に示されたライセンスサーバの構成を示す概略ブロック図である。

図６は、図１に示された携帯電話機の構成を示す概略ブロック図である。

図７は、図６に示されたメモリカードの構成を示す概略ブロック図である。

図８は、実施の形態１に従うデータ配信システムにおける配信動作を説明するための第１のフローチャートである。

図９は、実施の形態１に従うデータ配信システムにおける配信動作を説明するための第２のフローチャートである。

図１０は、実施の形態１に従う携帯電話機内において暗号化コンテンツデータを復号化し、音楽として外部に出力するための再生動作を説明するフローチャートである。

図１１は、実施の形態１に従う２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動を行なう処理を説明するための第１のフローチャートである。

図１２は、実施の形態１に従う２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動を行なう処理を説明するための第２のフローチャートである。

図１３は、実施の形態２に従うデータ配信システムのライセンスサーバの構成を示す概略ブロック図である。

図１４は、実施の形態２に従うデータ配信システムにおける携帯電話機の構成を示す概略ブロック図である。

図１５は、実施の形態２に従うデータ配信システムにおける配信動作を説明す

るためのフローチャートである。

図１６は、実施の形態２に従う携帯電話機における再生動作を説明するフローチャートである。

図１７は、実施の形態２に従うデータ配信システムにおける２つのメモリカード間の移動動作を説明するための第１のフローチャートである。

図１８は、実施の形態２に従うデータ配信システムにおける２つのメモリカード間における移動処理を説明する第２のフローチャートである。

図１９は、実施の形態３に従うメモリカードの構成を説明する概略ブロック図である。

図２０は、実施の形態３に従うデータ配信システムで使用される鍵データ等をまとめて説明する図である。

図２１は、実施の形態３に従うデータ配信システムにおける配信動作を説明するための第１のフローチャートである。

図２２は、実施の形態３に従うデータ配信システムにおける配信動作を説明するための第２のフローチャートである。

図２３は、実施の形態３のデータ配信システムにおいて、携帯電話機１１０における再生動作を説明するフローチャートである。

図２４は、実施の形態３に従う２つのメモリカード間におけるデータ等の移動処理を説明する第１のフローチャートである。

図２５は、実施の形態３に従う２つのメモリカード間におけるデータ等の移動処理を説明する第２のフローチャートである。

発明を実施するための最良の形態

以下、この発明の実施の形態によるデータ配信システムおよび当該データ配信システムで使用される記録装置、詳しくはメモリカードを図面を参照して詳しく説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

本発明の実施の形態では、携帯電話機網を介してデジタル音楽データを各携帯電話ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下

の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他のコンテンツデータ、たとえば画像情報等のコンテンツデータを、他の情報通信網を介して配信する場合にも適用することが可能なものである。

（実施の形態１）

図１を参照して、著作権の存在する音楽データを管理するライセンスサーバ１０は、所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、データを配信するための配信キャリア２０である携帯電話会社に、このような暗号化コンテンツデータを与える。一方、認証サーバ１２は、音楽データの配信を求めてアクセスしてきた携帯電話ユーザの携帯電話機およびメモリカード等が正規の機器であるか否かの認証を行なう。

配信キャリア２０は、自己の携帯電話網を通じて、各携帯電話ユーザからの配信要求（配信リクエスト）をライセンスサーバ１０に中継する。ライセンスサーバ１０は、配信リクエストがあると、認証サーバ１２により携帯電話ユーザの携帯電話機およびメモリカード等が正規の機器であることを確認し、要求されたコンテンツデータをさらに暗号化した上で配信キャリア２０の携帯電話網を介して、各携帯電話ユーザの携帯電話機に対してコンテンツデータを配信する。

図１においては、たとえば携帯電話ユーザ１の携帯電話機１００には、着脱可能なメモリカード１１０が装着される構成となっている。メモリカード１１０は、携帯電話機１００により受信された暗号化コンテンツデータを受取って、上記配信にあたって行なわれた暗号化については復号した上で、携帯電話機１００中の音楽再生部（図示せず）に与える。

さらに、たとえば携帯電話ユーザ１は、携帯電話機１００に接続したヘッドホン１３０等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

以下では、このようなライセンスサーバ１０と認証サーバ１２と配信キャリア２０と併せて、配信サーバ３０と総称することにする。

また、このような配信サーバ３０から、各携帯電話機等にコンテンツデータを伝送する処理を「配信」と称することとする。

このような構成とすることで、まず、メモリカード１１０を利用しないと、配

信サーバ３０からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

しかも、配信キャリア２０において、たとえば１曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア２０が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

しかも、このようなコンテンツデータの配信は、携帯電話機網というクローズなシステムを介して行なわれるため、インターネット等のオープンなシステムに比べて、著作権保護の対策を講じやすいという利点がある。

このとき、たとえばメモリカード１１２を有する携帯電話ユーザ２が自己の携帯電話機１０２により、配信サーバ３０から直接コンテンツデータの配信を受けることは可能である。しかしながら、相当量の情報量を有するコンテンツデータ等を携帯電話ユーザ２が直接配信サーバ３０から受信することとすると、この受信のために比較的長い時間を要してしまう場合がある。このような場合、既に当該コンテンツデータの配信を受けている携帯電話ユーザ１から、そのコンテンツデータをコピーできることを可能としておけば、携帯電話ユーザにとっての利便性が向上する。

図１に示すように、携帯電話ユーザ１が受信したコンテンツデータを、コンテンツデータそのものおよび当該コンテンツデータを再生可能とするために必要な情報とともに、携帯電話ユーザ２に対してコピーさせる場合をコンテンツデータの「移動」と呼ぶ。この場合に、携帯電話機１００および１０２を介して、メモリカード１１０と１１２との間で暗号化されたコンテンツデータ（音楽データ）および再生のために必要な情報（再生情報）が移動される。ここで、「再生情報」とは、後に説明するように、所定の暗号化方式に従って暗号化されたコンテンツデータを復号可能なライセンスキーと、著作権保護にかかわる情報であるライセンスＩＤやアクセス再生に関する制限情報等とを有する。

このような構成とすることによって、一旦配信サーバ３０より配信を受けたコンテンツデータについて受信者側での柔軟な利用が可能となる。

また、携帯電話機１００および１０２がＰＨＳ（Personal Handy Phone）である場合には、いわゆるトランシーバモードの通話が可能となっているので、このような機能を利用して、携帯電話ユーザ１と携帯電話ユーザ２との間における情報の移動を行なうことが可能である。

図１に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話ユーザ側で再生可能とするためにシステム上必要とされるのは、第１には、通信における暗号鍵を配信するための方式であり、さらに第２には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第３には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツデータ保護を実現する構成である。

本発明の実施の形態においては、特に、配信、再生および移動の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびコンテンツ再生回路（携帯電話機）に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

図２には、図１に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性が示される。

まず、配信サーバより配信されるデータについて説明する。Data は、音楽データ等のコンテンツデータである。コンテンツデータ Data には、ライセンスキーKc で復号可能な暗号化が施される。ライセンスキーKc によって復号可能な暗号化が施された暗号化コンテンツデータ {Data} Kc がこの形式で配信サーバ３０より携帯電話ユーザに配布される。

なお、以下においては、{Y} X という表記は、データ Y を、復号鍵 X により復号可能な暗号化を施したことを示すものとする。

さらに、配信サーバからは、暗号化コンテンツデータとともに、コンテンツデータに関するあるいはサーバアクセスに関する平文情報としての付加情報 Data-inf が配布される。また、再生情報としては、ライセンスキーKc の他に、コンテンツデータ Data を識別するためのコードであるコンテンツ ID およびライセンスの発行を特定できる管理コードであるライセンス ID や、利用者側からの指定に

よって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件AC に基づいて生成される、メモリのアクセスに対する制限に関する情報であるアクセス制限情報 AC１および再生回路における制御情報である再生回路制御情報 AC２等が存在する。なお、ライセンスＩＤ、コンテンツＩＤおよびアクセス制限情報 AC１を総括してライセンス情報と称し、このライセンス情報とライセンスキーKc および再生回路制限情報 AC2 を総括して再生情報とも称する。

次に図３を用いて、実施の形態１に従うデータ配信システムにおいて使用される認証および禁止クラスリストの運用のためのデータ、情報等の特性を説明する。

本発明の実施の形態においては、記録装置（メモリカード）やコンテンツ再生回路（携帯電話機）のクラスごとに、コンテンツデータの配信、再生および移動を禁止することができるように禁止クラスリスト CRL（Class Revocation List）の運用を行なう。以下では、必要に応じて記号 CRL によって禁止クラスリスト内のデータを表わすこともある。

禁止クラスリスト関連情報には、ライセンスの配信、再生および移動が禁止されるコンテンツ再生回路およびメモリカードのクラスをリストアップした禁止クラスリストデータ CRL が含まれる。

禁止クラスリストデータ CRL は、配信サーバ内で管理されるとともに、メモリカード内にも記録保持される。このような禁止クラスリストは、随時バージョンアップしデータを更新していく必要があるが、データの変更については、基本的には変更点のみを反映した差分データ CRL_dat の配信サーバ側より発生して、これに応じてメモリカード内の禁止クラスリスト CRL が書替えられる構成とする。また、禁止クラスリストのバージョンについては、CRL_ver をメモリカード側より出力し、これを配信サーバ側で確認することによってバージョン管理を実行する。また、禁止クラスリストのバージョンに代えて、禁止クラスリストの更新日時のような時間情報を用いても同様に運用することが可能である。

このように、禁止クラスリスト CRL を、配信サーバのみならずメモリカード内でおいても保持運用することによって、クラス固有すなわちコンテンツ再生回路およびメモリカードの種類に固有の復号鍵の破られた、コンテンツ再生回路およびメモリカードへのライセンスキーの供給を禁止する。このため、コンテンツ

再生回路ではコンテンツデータの再生が、メモリカードではコンテンツデータの移動が行なえなくなる。

このように、メモリカード内の禁止クラスリスト CRL は配信時に逐次データを更新する構成とする。また、メモリ回路内における禁止クラスリスト CRL の管理は、上位レベルとは独立にメモリカード内でタンパーレジスタントモジュール（Tamper Resistant Module）に記録する等によって、ファイルシステムやアプリケーションプログラム等によって上位レベルから禁止クラスリストデータ CRL を改ざんすることが不可能な構成とする。この結果、データに関する著作権保護をより強固なものとすることができる。

コンテンツ再生回路（携帯電話機）およびメモリカードにはクラス固有の公開暗号鍵 KPp（n）および KPmc（m）がそれぞれ設けられる。公開暗号鍵 KPp（n）および KPmc（m）はコンテンツ再生回路（携帯電話機）のクラス固有の秘密復号鍵 Kp（n）およびメモリカードのクラス固有の秘密復号鍵 Kmc（m）によってそれぞれ復号可能である。クラスとは、製造会社、種類、製造時のロットなどによって区別される、公開暗号鍵 KPmc（m）または KPp（n）を共有する単位である。これらの公開暗号鍵および秘密復号鍵は、携帯電話機のクラスごとおよびメモリカードのクラスごとに異なる値を持つ。

また、メモリカードおよび再生回路のクラス証明書として、Cp（n）および Cmc（m）がそれぞれ設けられる。ここで、自然数 m はメモリカードの、自然数 n はコンテンツ再生回路（携帯電話機）のクラスを区別するための番号を表わす。これらのクラス証明書は、メモリカードおよびコンテンツ再生部（携帯電話機）のクラスごとに異なる情報を有する。クラス固有の公開暗号鍵による暗号が破られた、すなわち、クラス固有の秘密復号鍵が漏洩したクラスは、禁止クラスリストにリストアップされてライセンス発行の禁止対象となる。

これらのメモリカードおよびコンテンツ再生部固有の公開暗号鍵およびクラス証明書は、認証データ｛KPmc（m）//Cmc（m）｝KPma および｛KPp（n）//Cp（n）｝KPma の形式で、出荷時にメモリカードおよび携帯電話機にそれぞれ記録される。KPma は配信システム全体で共通の認証鍵である。認証鍵 KPma を用いて、認証データ復号を行なうと、その復号結果から認証データの正当性が確認

できる。言い換えれば、認証鍵 KPma は、クラス固有の公開暗号鍵およびその証明書であるクラス証明書を承認するために用いられる鍵である。なお、認証データを作成するための暗号化は、認証鍵と対をなす非対称な秘密鍵によって行なわれる。

次に図４を用いて、図１に示したデータ配信システムにおいて暗号化に関わる鍵の特性をまとめて説明する。

メモリカード外とメモリカード間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、再生および移動が行なわれるごとにサーバ３０、携帯電話機１００または１０２、メモリカード１１０または１１２において生成される共通鍵 Ks１～Ks４が用いられる。

ここで、共通鍵 Ks１～Ks４は、サーバ、携帯電話機もしくはメモリカード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵 Ks１～Ks４を「セッションキー」とも呼ぶこととする。

これらのセッションキーKs１～Ks４は、各通信セッションごとに固有の値を有することにより、配信サーバ、携帯電話機およびメモリカードによって管理される。具体的には、セッションキーKs１は、配信サーバによって配信セッションごとに発生される。セッションキーKs２は、メモリカードによって配信セッションおよび移動（受信側）セッションごとに発生し、セッションキーKs３は、同様にメモリカードにおいて再生セッションおよび移動（送信側）セッションごとに発生する。セッションキーKs４は、携帯電話機において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンスキー等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

また、メモリカード１００内のデータ処理を管理するための鍵として、メモリカードという媒体ごとに設定される公開暗号鍵 KPm（i）（i：自然数）と、公開暗号鍵 KPm（i）で暗号化されたデータを復号することが可能なメモリカードごとに固有の秘密復号鍵 Km（i）が存在する。ここで、自然数 i は、各メモリカー

ドを区別するための番号を表わす。

その他の鍵としては、システムに共通の秘密鍵として、主としてライセンスキーKc の取得に利用される共通鍵方式における秘密鍵 Kcom が存在する。秘密鍵 Kcom は、配信サーバおよび携帯電話機の双方において保持され、ライセンスキーKc 等の暗号化および取得のための復号処理にそれぞれ使用される。

なお、共通鍵方式における秘密鍵 Kcom を、公開鍵方式における公開暗号鍵 Kpcom および秘密復号鍵 Kcom の組に置き換えて運用することも可能である。この場合には、公開暗号鍵 Kpcom は配信サーバに保持されてライセンスキーKc の暗号化に使用され、秘密復号鍵 Kcom は、携帯電話機に保持されてライセンスキーKc の取得に使用される。

図５を参照して、ライセンスサーバ１０は、コンテンツデータを所定の方式に従って暗号化したデータや、ライセンス ID 等の配信情報を保持するための情報データベース３０４と、各携帯電話ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース３０２と、禁止クラスリスト CRL を管理する CRL データベース３０６と、情報データベース３０４、課金データベース３０２および CRL データベース３０６からのデータをデータバス BS１を介して受取り、所定の処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリア２０とデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

データ処理部３１０は、データバス BS１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１５と、配信制御部３１５に制御されて、配信セッション時にセッションキーKs１を発生するためのセッションキー発生部３１６と、メモリカードおよび携帯電話機から送られてきた認証データ｛KPmc（m）//Cmc（m）｝KPma および｛KPp（n）//Cp（n）｝KPma を通信装置３５０およびデータバス BS１を介して受けて、KPma による復号処理を行なう復号処理部３１２と、セッションキー発生部３１６より生成されたセッションキーKs１を復号処理部３１２によって得られた公開暗号鍵 KPmc（m）を用いて暗号化して、データバス BS１に出力するための暗号化処理部３１８と、セッションキーKs１によって暗号化された上で送信されたデータをデータバス BS１を

より受けて、復号処理を行なう復号処理部３２０とを含む。

データ処理部３１０は、さらに、再生回路に共通な秘密鍵 Kcom を保持するKcom保持部３２２と、配信制御部３１５から与えられるライセンスキーKcおよび再生回路制御情報 AC２を再生回路共通の秘密鍵 Kcom で暗号化する暗号化処理部３２４と、暗号化処理部３２４から出力されたデータを復号処理部３２０によって得られたメモリカード固有の公開暗号鍵 KPm (i) によって暗号化するための暗号化処理部３２６と、暗号化処理部３２６の出力を、復号処理部３２０から与えられるセッションキーKs２によってさらに暗号化してデータバス BS１に出力するための暗号化処理部３２８とを含む。

なお、共通鍵 Kcom に代えて公開鍵方式における公開暗号鍵 Kpcom および秘密復号鍵 Kcom の組を用いる場合には、Kcom 保持部３２２に相当する部分に公開暗号鍵 Kpcom が保持される。さらに、暗号化処理部３２４によって、公開暗号鍵 Kpcom による暗号化が行なわれる。

ライセンスサーバ１０の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

図６を参照して、携帯電話機１００においては、携帯電話機のクラスを表わす自然数ｎ＝１、携帯電話機を個別に識別する自然数ｉ＝１とする。

携帯電話機１００は、携帯電話網により無線伝送される信号を受信するためのアンテナ１１０２と、アンテナ１１０２からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ１１０２に与えるための送受信部１１０４と、携帯電話機１００の各部のデータ授受を行なうためのデータバス BS２と、データバス BS２を介して携帯電話機１００の動作を制御するためのコントローラ１１０６とを含む。

携帯電話機１００は、さらに、外部からの指示を携帯電話機１００に与えるためのタッチキー部１１０８と、コントローラ１１０６等から出力される情報を携帯電話ユーザに視覚情報として与えるためのディスプレイ１１１０と、通常の通話動作において、データベース BS２を介して与えられる受信データに基づいて音声を再生するための音声再生部１１１２と、外部との間でデータの授受を行なうためのコネクタ１１２０と、コネクタ１１２０からのデータをデータバス BS

２に与え得る信号に変換し、または、データバス BS２からのデータをコネクタ１１２０に与え得る信号に変換するための外部インタフェース部１１２２とを含む。

携帯電話機１００は、さらに、配信サーバ３０からのコンテンツデータ（音楽データ）を記憶しかつ復号化処理するための着脱可能なメモリカード１１０と、メモリカード１１０とデータバス BS２との間のデータの授受を制御するためのメモリインタフェース１２００と、携帯電話機のクラスごとにそれぞれ設定される公開暗号鍵 KPp（1）およびクラス証明書 Cp（1）を認証鍵 KPma で復号することで認証可能な状態に暗号化したデータを保持する認証データ保持部１５００を含む。

携帯電話機１００は、さらに、携帯電話機（コンテンツ再生回路）のクラス固有の秘密復号鍵である Kp（1）を保持する Kp 保持部１５０２と、データバス BS２から受けたデータを Kp（1）によって復号しメモリカードによって発生されたセッションキーKs３を得る復号処理部１５０４と、メモリカード１１０に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード１１０との間でデータバス BS２上においてやり取りされるデータを暗号化するためのセッションキーKs４を乱数等により発生するセッションキー発生部１５０８と、生成されたセッションキーKs４を復号処理部１５０４によって得られたセッションキーKs３によって暗号化しデータバス BS２に出力する暗号化処理部１５０６と、データバス BS２上のデータをセッションキーKs４によって復号して出力する復号処理部１５１０とをさらに含む。

携帯電話機１００は、さらに、再生回路に共通に設定される秘密鍵 Kcom を保持する Kcom 保持部１５１２と、復号処理部１５１０が出力する｛Kc//AC２｝Kcom を秘密鍵 Kcom で復号しライセンスキーKc および再生回路制御情報 AC２を出力する復号処理部１５１４と、データバス BS２より暗号化コンテンツデータ｛Data｝Kc を受けて、復号処理部１５１４より取得してライセンスキーKc によって復号しコンテンツデータを出力する復号処理部１５１６と、復号処理部１５１６の出力を受けてコンテンツデータを再生するための音楽再生部１５１８と、音楽再生部１５１８と音声再生部１１１２の出力を受けて、動作モードに応じて

選択的に出力するための切換部１５２５と、切換部１５２５の出力を受けて、ヘッドホン１３０と接続するための接続端子１５３０とを含む。

なお、図６においては、説明の簡素化のため、携帯電話機のうち本発明の音楽データの配信および再生にかかわるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックに付いては、一部記載を省略している。

また、携帯電話ユーザの利便性を図るために、携帯電話機１００のうち、通話処理に関するブロックを除いた、図６において点線で囲まれる、コンテンツデータの配信および再生に関するブロック全体を音楽再生モジュール１５５０として、着脱可能なモジュール化する構成を採用することも可能である。

なお、共通鍵 Kcom に代えて公開鍵方式における公開暗号鍵 Kpcom および秘密復号鍵 Kcom の組を用いる場合には、Kcom 保持部１５１２に相当する部分に秘密復号鍵 Kcom が保持される。さらに、復号処理部１５１４によって、秘密復号鍵 Kcom による復号化が行なわれる。

携帯電話機１００の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

図７を参照して、公開暗号鍵 KPm (i) およびこれに対応する秘密復号鍵 Km (i) は、メモリカードごとに固有の値であるが、メモリカード１１０においては、この自然数 i＝１として取扱う。また、メモリカードのクラス固有の公開暗号鍵および秘密復号鍵として、KPmc (m) および Kmc (m) が設けられ、メモリカードのクラス証明書として Cmc (m) が設けられるが、メモリカード１１０においては、これらは自然数 m＝１でそれぞれ表わされるものとする。

したがって、メモリカード１１０は、認証データ {KPmc (１) //Cmc (１) } KPma を保持する認証データ保持部１４００と、メモリカードのクラスごとに設定されるの固有の復号鍵である Kmc (１) を保持する Kmc 保持部１４０２と、メモリカードごとに固有に設定される秘密復号鍵 Km (１) を保持する Km (１) 保持部１４２１と、Km (１) によって復号可能な公開暗号鍵 KPm (１) を保持する KPm (１) 保持部１４１６とを含む。

このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたラ

イセンスキーの管理をメモリカード単位で実行することが可能になる。

メモリカード１１０は、さらに、メモリインタフェース１２００との間で信号を端子１２０２を介して授受するデータバスBS３と、データバスBS３にメモリインタフェース１２００から与えられるデータから、メモリカードの種類ごとに固有の秘密復号鍵 Kmc（１）を Kmc（１）保持部１４０２から受けて、配信サーバ３０が配信セッションにおいて生成したセッションキーKs１、または他のメモリカードが移動セッションにおいて生成したセッションキーKs３を接点 Pa に出力する復号処理部１４０４と、KPma 保持部１４１４から認証鍵 KPma を受けて、データバス BS３に与えられるデータから KPma による復号処理を実行して復号結果を暗号化処理部１４１０に出力する復号処理部１４０８と、切換スイッチ１４４２によって選択的に与えられる鍵によって、切換スイッチ１４４４によって選択的に与えられるデータを暗号化してデータバス BS３に出力する暗号化処理部１４０６とを含む。

メモリカード１１０は、さらに、配信、再生および移動の各セッションにおいてセッションキーKs３を発生するセッションキー発生部１４１８と、セッションキー発生部１４１８の出力したセッションキーKs３を復号処理部１４０８によって得られる公開暗号鍵 KPp（n）もしくは KPmc（m）によって暗号化してデータバス BS３に送出する暗号化処理部１４１０と、BS３よりセッションキーKs３によって暗号化されたデータを受けてセッションキー発生部１４１８より得たセッションキーKs３によって復号し、復号結果をデータバス BS４に送出する復号処理部１４１２とを含む。

メモリカード１１０は、さらに、データバス BS４上のデータを他のメモリカードの公開暗号鍵 KPm(ｉ)（ｉ≠１）で暗号化する暗号化処理部１４２４と、データバス BS４上のデータを公開暗号鍵 KPm（１）と対をなすメモリカード１１０固有の秘密復号鍵 Km（１）によって復号するための復号処理部１４２２と、公開暗号鍵 KPm（１）で暗号化されている、ライセンスキーKc、再生回路制御情報 AC２およびライセンス情報（コンテンツ ID，ライセンス ID，アクセス制御情報 AC１）をデータバス BS４より受けて格納するとともに、暗号化コンテンツデータ {Data} Kc および付加情報 Data-inf をデータバス BS３より受けて格

納するためのメモリ１４１５とを含む。メモリ１４１５は、例えば半導体メモリによって構成される。

メモリカード１１０は、さらに、配信サーバより与えられる禁止クラスリストのバージョン更新のための差分データ CRL_dat によって逐次更新される禁止クラスリスト CRL を格納するための CRL 保持部１４３０と、復号処理部１４２２によって得られるライセンス ID、コンテンツ ID およびアクセス制限情報 AC１を保持するためのライセンス情報保持部１４４０と、データバス BS３を介して外部との間でデータ授受を行ない、データバス BS４との間で再生情報等を受けて、メモリカード１１０の動作を制御するためのコントローラ１４２０とを含む。

ライセンス情報保持部１４４０は、データバス BS４との間で、ライセンス情報（コンテンツ ID，ライセンス ID，アクセス制御情報 AC１）の授受が可能である。ライセンス情報保持部１４４０は、N個（N：自然数）のバンクを有し、各ライセンスに対応するライセンス情報をバンクごとに保持する。

なお、図７において、実線で囲んだ領域は、メモリカード１１０内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュール TRM に組込まれているものとする。このようなモジュールは、一般にはタンパーレジスタンスモジュールが用いられる。

もちろん、メモリ１４１５も含めて、モジュール TRM 内に組込まれる構成としてもよい。しかしながら、図７に示したような構成とすることで、メモリ１４１５中に保持されている再生に必要な再生情報は、いずれも暗号化されているデータであるため、第三者はこのメモリ１４１５中のデータのみでは、音楽を再生することは不可能であり、かつ高価なタンパーレジスタンスモジュール内にメモリ１４１５を設ける必要がないので、製造コストが低減されるという利点がある。

しかしながら、十分な TRM 領域が確保できるのであれば、ライセンス保持部 1440 に、復号して平文となったすべての再生情報（ライセンスキーKc、再生回路制御情報 AC2、ライセンスＩＤ、コンテンツＩＤおよびアクセス制限情報 AC1）を保持しても問題はなく、同様な効果を得ることができる。

次に、本発明の実施の形態１に従うデータ配信システムの各セッションにおけ

これらの公開暗号鍵が無効である場合には、処理を終了（ステップＳ１７０）する（ステップＳ１１０）。

また、認証データ｛KPmc（１）｝KPma｛および認証データ｛KPp（１）｝KPmaは、それぞれが認証鍵KPmaによって復号することで、その正当性が判断可能な暗号化が施されているため、認証サーバ１２に対して照会せず、ライセンスサーバ１０の配信制御部３１５が、認証鍵KPmaによる復号結果から独自に認証を行なう構成としてもよい。

照会の結果、正規の機器であることが認識されると、配信制御部３１５は、次に、メモリカード１１０および携帯電話機１００のコンテンツ再生回路のクラス証明書Cmc（１）およびCp（１）が禁止クラスリストCRLにリストアップされているかどうかをCRLデータベース３０６に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する（ステップＳ１７０）。

一方、メモリカード１１０および携帯電話機１００の再生回路のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップＳ１１２）。

照会の結果、正規のクラス証明書を持つメモリカードと再生回路とを備える携帯電話機からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、配信サーバ３０において、セッションキー発生部３１６は、配信のためのセッションキーKs１を生成する。セッションキーKs１は、復号処理部３１２によって得られたメモリカード１１０に対応する公開暗号鍵KPmc（１）によって、暗号化処理部３１８によって暗号化される（ステップＳ１１４）。

暗号化されたセッションキーKs１は、｛Ks１｝Kmc（１）として、データバスBS１および通信装置３５０を介して外部に出力される（ステップＳ１１６）。

携帯電話機１００が、暗号化されたセッションキー｛Ks１｝Kmc（１）を受信すると（ステップＳ１１８）、メモリカード１１０においては、メモリインタフェース１２００を介して、データバスBS３に与えられた受信データを、復号処理部１４０４が、保持部１４０２に保持されるメモリカード１１０固有の秘密復

号鍵 Kmc（１）により復号処理することにより、セッションキーKs１を復号し抽出する（ステップＳ１２０）。

コントローラ１４２０は、配信サーバ３０で生成されたセッションキーKs１の受理を確認すると、セッションキー発生部１４１８に対して、メモリカードにおいて配信動作時に生成されるセッションキーKs２の生成を指示する。

また、配信セッションにおいては、コントローラ１４２０は、メモリカード１１０内の CRL 保持部１４３０に格納されている禁止クラスリストの状態（バージョン）に関連する情報として、リストのバージョンデータ CRL_ver を CRL 保持部１４３０から抽出してデータバス BS４に出力する。

暗号化処理部１４０６は、切換スイッチ１４４２の接点 Pa を介して復号処理部１４０４より与えられるセッションキーKs１によって、切換スイッチ１４４４および１４４６の接点を順次切換えることによって与えられるセッションキーKs２、公開暗号鍵 KPm（１）および禁止クラスリストのバージョンデータ CRL_ver を１つのデータ列として暗号化して、｛Ks２//KPm（１）//CRL_ver｝Ks１をデータバス BS３に出力する（ステップＳ１２２）。

データバス BS３に出力された暗号データ｛Ks２//KPm（１）//CRL_ver｝Ks１は、データバス BS３から端子１２０２およびメモリインタフェース１２００を介して携帯電話機１００に出力され、携帯電話機１００から配信サーバ３０に送信される（ステップＳ１２４）。

配信サーバ３０は、暗号化データ｛Ks２//KPm（１）//CRL_ver｝Ks１を受信して、復号処理部３２０においてセッションキーKs１による復号処理を実行し、メモリカード１１０で生成されたセッションキーKS２、メモリカード１１０固有の公開暗号鍵 Kpm（１）およびメモリカード１１０における禁止クラスリストのバージョンデータ CRL_ver を受理する（ステップＳ１２６）。

禁止クラスリストのバージョン情報 CRL_ver は、データバス BS１を介して配信制御部３１５に送られ、配信制御部３１５は、受理したバージョンデータ CRL_ver に従って、当該 CRL_ver のバージョンと CRL データベース３０６内の禁止クラスリストデータの現在のバージョンとの間の変化を表わす差分データ CRL_dat を生成する（ステップＳ１２８）。

さらに、配信制御部３１５は、ステップＳ１０６で取得したコンテンツ ID およびライセンス購入条件 AC に従って、ライセンス ID、アクセス制限情報 AC1 および再生回路制御情報 AC２を生成する（ステップＳ１３０）。さらに、暗号化コンテンツデータを復号するためのライセンスキーKc を情報データベース３０４より取得する（ステップＳ１３２）。

図９を参照して、配信制御部３１５は、取得したライセンスキーKc および再生回路制御情報 AC２を暗号化処理部３２４に与える。暗号化処理部３２４は、Kcom 保持部３２２より得られる、秘密鍵 Kcom によって、ライセンスキーKc および再生回路制御情報 AC２を暗号化する（ステップＳ１３４）。

暗号化処理部３２４が出力する暗号化データ｛Kc//AC２｝Kcom と、配信制御部３１５が出力するライセンス ID、コンテンツ ID およびアクセス制限情報 AC１とは、暗号化処理部３２６によって、復号処理部３２０によって得られたメモリカード１１０固有の公開暗号鍵 KPm（１）によって暗号化される（ステップＳ１３６）。暗号化処理部３２８は、暗号化処理部３２６の出力と、配信制御部３１５が出力する禁止クラスリストのバージョンの更新情報 CRL_dat とを受けて、メモリカード１１０において生成されたセッションキーKs２によって暗号化する。暗号化処理部３２８より出力された暗号化データは、データバス BS１および通信装置３５０を介して携帯電話機１００に送信される（ステップＳ１３８）。

このように、配信サーバおよびメモリカードでそれぞれ生成される暗号鍵をやりとりし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号データを相手方に送信することによって、それぞれの暗号データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

携帯電話機１００は、送信された暗号化データ｛｛｛｛KC//AC２｝Kcom//ライセンス ID//コンテンツ ID//AC１｝Km（１）//CRL_dat｝Ks2 を受信し（ステップＳ１４０）、メモリカード１１０においては、メモリインタフェース１２００を介して、データバス BS３に与えられた受信データを復号処理部１４１２によって復号する。復号処理部１４１２は、セッションキー発生部１４１８から与え

られたセッションキーKs２を用いてデータバス BS３の受信データを復号しデータバスBS４に出力する（ステップＳ１４２）。

この段階で、データバス BS４には、Km（１）保持部１４２１に保持される秘密復号鍵 Km（１）で復号可能な暗号化再生情報｛｛KC//AC２｝Kcom//ライセンス ID//コンテンツ ID//AC１｝Km（１）と、CRL_dat とが出力される。コントローラ１４２０の指示によって、暗号化再生情報｛｛Kc//AC２｝Kcom//ライセンス ID//コンテンツ ID//AC１｝Km（１）は、メモリ１４１５に記録される（ステップＳ１４４）。一方、｛｛KC//AC２｝Kcom//ライセンス ID//コンテンツ ID//AC１｝Km（１）は、復号処理部１４２２において、秘密復号鍵 Km（１）によって復号され、ライセンス情報であるライセンス ID、コンテンツ ID およびアクセス制限情報 AC１のみが受理される（ステップＳ１４６）。

コントローラ１４２０は、受理した CRL_dat に基づいて、CRL 保持部１４３０内の禁止クラスリストデータ CRL およびそのバージョンを更新する（ステップＳ１４８）。さらに、ライセンス ID、コンテンツ ID およびアクセス制限情報 AC１については、ライセンス情報保持部１４４０に記録される（ステップＳ１５０）。

ステップＳ１５０までの処理がメモリ回路で正常に終了した段階で、携帯電話機１００から配信サーバ３０にコンテンツデータの配信要求がなされる（ステップＳ１５２）。

配信サーバ３０は、コンテンツデータの配信要求を受けて、情報データベース３０４より、暗号化コンテンツデータ｛Data｝Kc および付加情報 Data-inf を取得して、これらのデータをデータバス BS１および通信装置３５０を介して出力する（ステップＳ１５４）。

携帯電話機１００は、｛Data｝Kc//Data-inf を受信して、暗号化コンテンツデータ｛Data｝Kc および付加情報 Data-inf を受理する（ステップＳ１５６）。暗号化コンテンツデータ｛Data｝Kc および付加情報 Data-inf はメモリインタフェース１２００および端子１２０２を介してメモリカード１１０のデータバス BS３に伝達される。メモリカード１１０においては、受信した暗号化コンテンツデータ｛Data｝Kc および付加情報 Data-inf がそのままメモリ１４１５に記録される（ス

テップＳ１５８）。

さらに、メモリカード１１０から配信サーバ３０へは、配信受理の通知が送信され（ステップＳ１６０）、配信サーバ３０で配信受理を受信すると（ステップＳ１６２）、課金データベース３０２への課金データの格納等を伴って、配信終了の処理が実行され（ステップＳ１６４）、全体の処理が終了する（ステップＳ１７０）。

このようにして、携帯電話機１００のコンテンツ再生部およびメモリカード１１０が正規の機器であること、同時に、それぞれがクラス証明書 Cp(１)および Cmc(１)とともに暗号化して送信できた公開暗号鍵 Kp(１)および Kmc(１)が有効であることを確認した上で、それぞれのクラス証明書 Cp(１)および Cmc(１)が禁止クラスリスト、すなわち、公開暗号鍵 Kp(１)および Kmc(１)による暗号化が破られたクラス証明書リストに記載されていない機器からの配信要求に対してのみコンテンツデータを配信することができ、不正な機器および暗号化の破られた機器への配信を禁止することができる。

次に図１０のフローチャートを用いて、携帯電話機１００内において、メモリカード１１０に保持された暗号化コンテンツデータから音楽を再生し、外部に出力するための再生動作（以下、再生セッションともいう）を説明する。

図１０を参照して、携帯電話機のタッチキー部１１０８からの携帯電話ユーザ１の指示により、再生リクエストが生成される（ステップＳ２００）。携帯電話機１００は、再生リクエストの生成に応じて、認証データ保持部１５００より、認証鍵 KPma で復号することで認証可能な認証データ｛KPp（１）//Cp（１）｝KPma をデータバス BS２に出力する（ステップＳ２０２）。

認証データ｛KPp（１）//Cp（１）｝KPma は、データバス BS２およびメモリインタフェース１２００を介してメモリカード１１０に伝達される。

メモリカード１１０においては、端子１２０２を介してデータバス BS３に伝達される認証データ｛KPp（１）//Cp（１）｝KPma は、復号処理部１４０８に取込まれる。復号処理部１４０８は、KPma 保持部１４１４から認証鍵 KPma を受けて、データバス BS３のデータを復号処理し、コンテンツ再生部すなわち携帯電話機１００の種類に固有の公開暗号鍵 KPp（１）およびクラス証明書 Cp

（1）を得る。コントローラ１４２０は、データバス BS３を介して公開暗号鍵 KPp（1）およびクラス証明書 Cp（1）を受理する（ステップＳ２０４）。

コントローラ１４２０は、復号処理部１４０８の復号結果に基づいて、受理した携帯電話機１００のコンテンツ再生回路の認証作業を行ない、携帯電話機１００のコンテンツ再生回路が承認されたものである場合には処理を次のステップ（ステップＳ２０８）に進める（ステップＳ２０６）。一方、携帯電話機１００のコンテンツ再生回路が非承認である場合には、再生セッションの処理を終了する（ステップＳ２４０）。

携帯電話機１００が承認された機器であることを確認した場合には、引続き、携帯電話機１００のコンテンツ再生部のクラス証明書 Cp（1）が禁止クラスリスト CRL にリストアップされているかの判定が実行される（ステップＳ２０８）。ステップＳ２０８においては、携帯電話機１００のクラスが禁止クラスリストＣＲＬにリストアップされているクラスに含まれる場合には、再生セッションの処理を終了する（ステップＳ２４０）。

一方、携帯電話機１００のクラスが、禁止クラスリスト CRL に含まれない場合においては、次のステップに処理を進め、コントローラ１４２０は、セッションキー発生部１４１８に対して、再生セッションにおけるセッションキーKs３の生成をデータバス BS４を介して指示する。セッションキー発生部１４１８によって生成されたセッションキーKs３は、暗号化処理部１４１０に送られる。暗号化処理部１４１０は、復号処理部１４０８によって得られた携帯電話機１００の公開暗号鍵 KPp（1）によってセッションキーKs３を暗号化し公開暗号鍵 KPp（1）に対応する秘密復号鍵 Kp（1）で復号可能な暗号化データ｛Ks３｝Kp（1）をデータバス BS３に出力する（ステップＳ２１０）。

携帯電話機１００は、端子１２０２およびメモリインタフェース１２００を介して、データバス BS に暗号化データ｛Ks３｝Kp（1）を受ける。暗号化データ｛Ks３｝Kp（1）は、復号処理部１５０４によって復号され、メモリカード１１０で生成されたセッションキーKs３が受理される（ステップＳ２１２）。

コントローラ１１０６は、セッションキーKs３の受理に応じて、セッションキー発生部１５０８に対して、再生セッションにおいて携帯電話機１００で生成

されるセッションキーKs４の発生をデータバス BS２を介して指示する。生成されたセッションキーKs４は暗号化処理部１５０６に送られ、復号処理部１５０４によって得られたセッションキーKs３によって暗号化された｛Ks４｝Ks３がデータバスBS２に受理される（ステップＳ２１４）。

暗号化されたセッションキー｛Ks４｝Ks３は、メモリインタフェース１２００を介してメモリカード１１０に伝達される。メモリカード１１０においては、データバス BS３に伝達される暗号化されたセッションキー｛Ks４｝Ks３を復号処理部１４１２によって復号し、携帯電話機で生成されたセッションキーKs４を受理する（ステップＳ２１６）。セッションキーKs４の受理に応じて、コントローラ１４２０は、ライセンス情報保持部１４４０内の対応するアクセス制限情報 AC１を確認する（ステップＳ２１８）。

ステップＳ２１８においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報 AC１を確認することにより、既に再生不可の状態である場合には再生セッションを終了し（ステップＳ２４０）、再生回数に制限がある場合にはアクセス制限情報 AC１のデータを更新し再生可能回数を更新した後に次のステップに進む（ステップＳ２２０）。一方、アクセス制限情報 AC１によって再生回数が制限されていない場合においては、ステップＳ２２０はスキップされ、再生制御情報 AC１は更新されることなく処理が次のステップ（ステップＳ２２２）に進行される。

また、ライセンス情報保持部１４４０内にリクエスト曲の当該コンテンツ ID が存在しない場合においても、再生不可の状態にあると判断して、再生セッションを終了する（ステップＳ２４０）。

ステップＳ２１８において、当該再生セッションにおいて再生が可能であると判断された場合には、メモリに記録された再生リクエスト曲のライセンスキー Kc を含む再生情報の復号処理が実行される。具体的には、コントローラ１４２０の指示に応じて、メモリ１４１５からデータバス BS４に読出された暗号化再生情報｛｛Kc//AC２｝Kcom//ライセンス ID//コンテンツ ID//AC１｝Km（１）を復号処理部１４２２がメモリカード１１０固有の秘密復号鍵 Km（１）によって復号し、共通の秘密鍵 Kcom によって復号可能な暗号化データ｛Kc//AC２｝

Kcom がデータバス BS４上に得られる（ステップＳ２２２）。

得られた暗号化データ｛Kc// AC２｝Kcom は、切換スイッチ１４４４の接点 Pd を介して暗号化処理部１４０６に送られる。暗号化処理部１４０６は、切換スイッチ１４４２の接点 Pb を介して復号処理部１４１２より受けたセッションキーKs４によってデータバス BS４から受けた暗号化データをさらに暗号化し、｛｛Kc//AC２｝Kcom｝Ks４をデータバス BS３に出力する（ステップＳ２２４）。

データバス BS３に出力された暗号化データは、メモリインタフェース１２００を介して携帯電話機１００に送出される。

携帯電話機１００においては、メモリインタフェース１２００を介してデータバス BS２に伝達される暗号化データ｛｛Kc//AC２｝Kcom｝Ks４を復号処理部１５１０によって復号処理を行ない、暗号化されたライセンスキーKc および再生回路制御情報 AC２を受理する（ステップＳ２２６）。復号処理部１５１４は、暗号化データ｛Kc//AC２｝Kcom を、Kcom 保持部１５１２から受けた再生回路に共通の秘密鍵 Kcom によって復号し、ライセンスキーKc および再生回路制御情報 AC２を受理する（ステップＳ２２８）。復号処理部１５１４は、ライセンスキーKc を復号処理部１５１６に伝達し、再生回路制御情報 AC２をデータバス BS２に出力する。

コントローラ１１０６は、データバス BS２を介して、再生回路制御情報ＡＣ２を受理して再生の可否の確認を行なう（ステップＳ２３０）。

ステップＳ２３０においては、再生回路制御情報ＡＣ２によって再生不可と判断される場合には、再生セッションは終了される（ステップＳ２４０）。一方、再生可能である場合には、メモリカード１１０よりメモリに記録されたリクエスト曲の暗号化されたコンテンツデータ｛Data｝Kc がデータバス BS３に出力され、メモリインタフェース１２００を介して携帯電話機１００に伝達される（ステップＳ２３２）。

携帯電話機１００においては、メモリカード２１０から出力されデータバス BS２に伝達された暗号化コンテンツデータ｛Data｝Kc を復号処理部１５１６においてライセンスキーKc によって復号し、平文化されたコンテンツデータ Data を得ることができる（ステップＳ２３４）。復号された平文化コンテンツデータ

Data は音楽再生部１５１８によって音楽信号に変換され（ステップ２３０）、混合部１５２５および端子１５３０を介して外部に再生された音楽を出力することによって処理が終了する（ステップＳ２４０）。

このような構成とすることで、メモリカード１１０側において、コンテンツ再生回路である携帯電話機１００のクラスを確認し、禁止クラスリストにリストアップされているクラスに対しては、再生処理を禁止することが可能となる。

再生セッションにおいても、携帯電話機１００およびメモリカード１１０でそれぞれ生成される暗号鍵をやりとりし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信する。この結果、配信セッション同様、再生セッションにおいても、データのそれぞれの送受信において事実上の相互認証を行なうことができ、データ配信システムのセキュリティーを向上させることができる。

次に図１１および図１２のフローチャートを用いて、２つのメモリカード１１０および１１２の間で携帯電話機１００および１０２を介してコンテンツデータおよびキーデータ等の移動を行なう処理を説明する。

図１１および図１２においては、携帯電話機１００およびメモリカード１１０についてのクラスを識別するための自然数をそれぞれｍ＝１およびｎ＝１とし、携帯電話機１０２およびメモリカード１１２についてのクラスを認識するため自然数をそれぞれｍ＝２およびｎ＝２とする。また、メモリカード１１０および１１２を識別するための自然数ｉは、それぞれｉ＝１およびｉ＝２であるものとする。

図１１および図１２においては、携帯電話機１００およびメモリカード１１０が送信側であり、携帯電話機１０２およびメモリカード１１２が受信側であるものとする。また、携帯電話機１０２も、メモリカード１１０と同様の構成を有するメモリカード１１２が装着されているものとする。以下、メモリカード１１２の各構成部分については、メモリカード１１０の対応する部分と同一の符号を用いて説明する。

図１１を参照して、まず送信側である携帯電話ユーザ１により、携帯電話機１００からタッチキー部１１０８のキーボタンの操作等によって、コンテンツ移動

リクエストがなされる。（ステップＳ３００）。

生成された移動リクエストは、受信側である携帯電話ユーザ２の携帯電話機１２０を介してメモリカード１１２に伝達される。メモリカード１１２においては、認証データ保持部１５００より、メモリカード１１２に対応する公開暗号鍵 KPmc（２）およびクラス証明書 Cmc（２）が暗号化された認証データ｛KPmc（２）//Cmc（２）｝KPma が出力される（ステップＳ３０２）。

メモリカード１１２の認証データ｛KPmc（２）//Cmc（２）｝KPma は、携帯電話ユーザ２の携帯電話機１２０から送信され、携帯電話ユーザ１の携帯電話機１１０を経由してメモリカード１１０に受信される（ステップＳ３０４）。

メモリカード１１０においては、復号処理部１４０８によって、メモリカード１１２の認証データが復号され、メモリカード１１２に関する公開暗号鍵 KPmc（２）およびクラス証明書 Cmc（２）が受理される（ステップＳ３０６）。コントローラ１４２０は、データバス BS３を介して受理された認証処理部１４０８の復号結果に基づいて、認証作業を実行する（ステップＳ３０８）。まず、コントローラ１４２０は、メモリカード１１２に関する認証データ｛KPmc（２）//Cmc（２）｝KPma を認証鍵 KPma によって復号した復号結果から、認証データ｛KPmc（２）//Cmc（２）｝KPma が正規の機器から出力された認証データであることを確認し、正規の機器から出力された有効な認証データである場合には、公開暗号鍵 KPmc（２）およびクラス証明書 Cmc（２）を承認し、次のステップＳ３１０を実行する。正規の機器から出力されたことが確認できない無効な認証データである場合には、移動セッションを終了する（ステップＳ３６０）。

認証の結果、有効な認証データである場合には、コントローラ１４２０は、引続き、メモリカード１１２のクラス証明書 Cmc（２）が禁止クラスリストに含まれるか否かの判定を実行する（ステップＳ３１０）。メモリカード１１２に関するクラス証明書 Cmc（２）が禁止クラスリストに含まれる場合においては、移動セッションはこの段階で終了される（ステップＳ３６０）。一方、メモリカード１１２の属するクラスが禁止クラスリストに含まれない場合においては、移動セッションを実行するために次のステップＳ３１２に処理が進行する。

この場合においては、コントローラ１４２０は、セッションキー発生部１４１

8に対して、移動セッション時に送信側で発生されるセッションキーKs３の出力を指示する。セッションキーへ発生部１４１８によって生成されたセッションキーKs３は、暗号化処理部１４１０に伝達される。暗号化処理部１４１０は、さらに、ステップＳ３０６において復号処理部１４０８によって復号されたメモリカード１１２の公開暗号鍵 KPmc（２）によってセッションキーKs３を暗号化する。これにより、暗号化されたセッションキー｛Ks３｝Kmc（２）がデータバスBS３に出力される（ステップＳ３１４）。データバスBS３に出力された｛Ks３｝Kmc（２）｝は、メモリインタフェース１２００、携帯電話機１００、および携帯電話機１０２を介してメモリカード１１２に伝達される。

メモリカード１１２は、メモリカード１１０から出力された｛Ks３｝Kmc（２）を受けて、復号処理部１４０４によってメモリカード１１２に対応する秘密復号鍵 Kmc（２）による復号処理を実行し、送信側のメモリカード１１０によって生成されたセッションキーKs３を受理する（ステップＳ３１６）。

メモリカード１１２のコントローラ１４２０は、セッションキーKs３の受理に応じて、セッションキー発生部１４１８に対して、移動セッションにおいて受信側で発生されるべきセッションキーKs２の生成を指示する。生成されたセッションキーKs２は、切換スイッチ１４４６中の接点 Pf および切換スイッチ１４４４中の接点Pcを経由して暗号化処理部１４０６に伝達される。

暗号化処理部１４０６は、復号処理部１４０４からステップＳ３１６で得られたセッションキーKs３を受けて、切換スイッチ１４４４の接点 Pc と切換スイッチ１４４６の接点の切換によって得られるセッションキーKs２と公開暗号鍵 KPm（２）をセッションキーKs３によって暗号化し、｛Ks２//KPm（２）｝Ks３をデータバスBS３に出力する（ステップＳ３１８）。データバスBS３に出力された暗号化データ｛Ks２//KPm（２）｝Ks３は、携帯電話機１０２および１００を介してメモリカード１１０のデータバスBS３に伝達される。

メモリカード１１０においては、データバス BS３に伝達された暗号化データを符号処理部１４１２によってセッションキーKs３を用いて復号し、メモリカード１１２に関するセッションキーKs２および公開暗号鍵 KPm（２）を受理する（ステップＳ３２０）。

メモリカード１１０のコントローラ１４２０は、セッションキーKs２および公開暗号鍵 KPm（２）の受理に応じて、ライセンス情報保持部１４４０内のアクセス制限情報 AC１の確認を実行する。アクセス制御情報 AC１を確認した結果、ライセンスの移動が不可である場合には、この段階で移動を終了する（ステップＳ３６０）。一方、アクセス制限情報 AC１を確認した結果、移動セッションが許可されている場合には、次のステップに進み（ステップＳ３２２）、ライセンス情報保持部１４４０より対応するコンテンツ ID およびライセンス ID を取得し、さらにライセンス情報保持部１４４０内のアクセス制御情報 AC1 を更新して、以降の再生および移動の禁止を記録する（ステップＳ３２４）。これに対応して、再生セッションおよび移動セッションにおいて当該アクセス制御情報 AC1 を確認して処理が行なわれ、以降のそれぞれのセッションが禁止される。

さらに、コントローラ１４２０は、移動するコンテンツデータに対応したセッションキーKc および再生情報に関する暗号化再生情報｛｛Kc//AC２｝Kcom//ライセンス ID//コンテンツ ID//AC１｝Km（１）の出力をメモリ１４１５に対して指示する。メモリ１４１５から出力された暗号化再生情報｛｛Kc//AC２｝Kcom//ライセンス ID//コンテンツ ID//AC１｝Km（１）は、復号処理部１４２２によって復号化され、｛Kc//AC２｝Kcom がデータバス BS４上に得られる（ステップＳ３２６）。

ステップＳ３２４でライセンス情報保持部１４４０から取得されたライセンス ID、コンテンツ ID およびアクセス制限情報 AC１と、ステップＳ３２６で得られた｛Kc//AC２｝Kcom は、データバス BS４から暗号化処理部１４２４に取込まれて暗号化される。暗号化処理部１４２４は、ステップＳ３２０において復号処理部１４１２で得られた受信側メモリカード１１２固有の公開暗号鍵 KPm（２）によって、これらのデータを暗号化し、暗号化再生情報｛｛Kc//AC２｝Kcom//ライセンス ID//コンテンツ ID//AC１｝Km（２）を出力する（ステップＳ３２８）。

図１２を参照して、データバス BS４に出力された暗号化再生情報｛｛Kc//AC２｝Kcom//ライセンス ID//コンテンツ ID//AC１｝Km（２）は、切換スイッチ１４４４中の接点 Pd を介して暗号化処理部１４０６に伝達される。暗号化処理部

１４０６は、復号処理部１４１２によって得られたメモリカード１１２の生成したセッションキーKs２を切換スイッチ１４４２の接点 Pb を介して受けて、接点 Pd より受けたデータをセッションキーKs２によって暗号化する。

暗号化処理部１４０６は、暗号化データ｛｛｛Kc//AC２｝Kcom//ライセンス ID//コンテンツ ID//AC１｝Km（２）｝Ks２をデータバス BS３に出力する（ステップＳ３３０）。ステップＳ３３０においてデータバス BS３に出力された暗号化再生情報は、携帯電話機１００および１０２を介して、移動セッションの受信側であるメモリカード１１２に伝達される。

メモリカード１１２においては、復号処理部１４１２においてセッションキー発生部１４１８によって生成されたセッションキーKs２による復号が実行され、暗号化再生情報｛｛｛Kc//AC２｝Kcom//ライセンス ID//コンテンツ ID//AC１｝Km（２）が受理される（ステップＳ３３２）。

暗号化再生情報｛｛Kc//AC２｝Kcom//ライセンス ID//コンテンツ ID//AC１｝Km（２）は、メモリ１４１５に記録される（ステップＳ３３４）。さらに、復号処理部１４２２において、メモリカード１１２に固有の秘密復号鍵 Km（２）による復号処理を実行することにより、ライセンス ID、コンテンツ ID およびアクセス制限情報 AC１が受理される（ステップＳ３３６）。

復号処理部１４２２によって得られたライセンス ID、およびコンテンツ ID およびアクセス制限情報 AC１は、データバス BS４を介してライセンス情報保持部１４４０に記録される（ステップＳ３３８）。

このようにして、ステップＳ３３８までの処理が正常に終了することによって、ライセンスキーKc を含む再生情報が移動されたことに応答して、携帯電話機１０２を介してコンテンツデータの複製要求がさらに行なわれる（ステップＳ３４０）。

コンテンツデータの複製要求は携帯電話機１００を経由してメモリカード１１０に伝達され、これに応答して、メモリカード１１０中のメモリ１４１５より対応する暗号化コンテンツデータ｛Data｝Kc と付加情報 Data-inf とがデータバス BS３に出力される（ステップＳ３４２）。

データバス BS３に出力されたこれらのデータは、携帯電話機１００および携

帯電話機１０２を介してメモリカード１１２に伝達され、メモリカード１１２中のメモリ１４１５に記録される（ステップＳ３４４）。

暗号化コンテンツデータ {Data} Kc および付加情報 Data-inf の記録が終了すると、携帯電話機１０２を介して移動受理が送信される（ステップＳ３４６）。

これにより、メモリカード１１２および対応する携帯電話機１０２において正常に再生セッションが実行されれば、携帯電話機１０２によって、メモリカード１１２に記録された暗号化コンテンツデータを再生して音楽を聴取することが可能となる。

送信側の携帯電話機１００においては、携帯電話機１０２から送信された移動受理を受信して（ステップＳ３４８）、コンテンツデータの消去もしくは保持のいずれかをキー１１０８より入力する（ステップＳ３５０）。本発明の実施の形態に従うデータ配信システムにおいては、利用者のライセンス数や再生可能回数に応じて再生が可能であるか否かは、アクセス制限情報 AC1 に応じて再生セッションによって判断されるため、携帯電話機１００側において、既に再生が不可能となった場合には、これ以上、暗号化コンテンツデータ等を保持する必要がない。

したがって、このような場合には、タッチキー部１１０８よりコンテンツデータの消去を指示することにより、メモリカード１１０内のメモリ１４１５において、対応する暗号化コンテンツデータ {Data} Kc、付加情報 Data-inf を消去することができる（ステップＳ３５４）。なお、ライセンス情報保持部１４４０内に記録された対応するライセンス情報は、ステップＳ３２４にてアクセス制御情報 AC1 が更新され、再生セッションおよび移動セッションを禁止しているため、消去と同じ状態になっている。なお、この状態にある再生情報に対して、新たなコンテンツデータに対する再生情報の配信あるいは移動を受けた際に、上書きが許可されている。

一方、暗号化コンテンツデータ等の保持が指示された場合においては、ステップＳ３５４はスキップされ、移動処理はこの段階で終了する（ステップＳ３５６）。

暗号化コンテンツデータがメモリ１４１５に記録された状態では、新たに配信

サーバ３０をアクセスし、再生情報の配信のみを受ければ、再び暗号化コンテンツデータを再生して音楽を聴取することができるようになる。再生情報のみの配信処理は、図８および図９のフローチャートには図示されていないが、コンテンツデータの授受に関するステップＳ１５２、Ｓ１５４、Ｓ１５６およびＳ１５８を行なわない処理であり、その他については、すでに説明した配信動作と同様であるので説明は繰り返さない。

正常に移動セッションが行なわれた場合の移動処理終了（ステップＳ３５６）もしくは認証および禁止クラスリストのチェック等によって移動セッションが中止された場合にはステップＳ３０８、Ｓ３１０およびＳ３２２からスキップされて移動セッション全体の処理が終了する（Ｓ３６０）。

このような構成とすることにより、移動セッションにおいても、受信側の携帯電話機に装着されたメモリカードが正規のメモリカードであるか否か、およびクラス証明書が禁止クラスリストの対象であるか否かを事前にチェックした後に、ライセンスキーやコンテンツデータの移動を実行する構成とするので、クラス固有の鍵が破られた再生回路（携帯電話機）もしくはメモリカードに対するコンテンツデータの移動の禁止を行なうことができる。

なお、実施の形態１においては、禁止クラスリストを運用することによって、データの配信、再生および移動を携帯電話機およびメモリカードのクラスごとに禁止することが可能な構成について説明したが、禁止クラスリストに代えて、許可クラスリスト CPL（Class Permission List）を運用することによって、許可クラスリストにリストアップされたクラスのメモリカードおよび携帯電話機に対してこれらのセッションを有効とする構成も可能である。

この場合には、ライセンスサーバ１０においては、ＣＲＬデータベース３０６に相当する部分で許可クラスリスト CPL を保持し、メモリカード１１０においては、ＣＲＬ保持部１４３０に相当する部分で許可クラスリスト CPL を格納すればよい。

さらに、許可クラスリスト CPL による運用を行なう場合には、配信セッションにおけるステップＳ１１２（図８）、再生セッションにおけるステップＳ２０８（図１０）および移動セッションにおけるステップＳ３１０（図１１）におけ

る含む／含まないの判定を逆にする動作フローを採用すればよい。また、許可クラスリストの運用についても、メモリカード内の CPL データの更新は、コンテンツデータ配信時あるいはユーザの要求によって、配信サーバ３０によって出力される、禁止クラスリストの運用におけるバージョンデータ CRL_ver および差分データ CRL_dat に相当する許可クラスリストの差分データおよびバージョンの更新情報に基づいてメモリカード内の CPL リストを書換える構成とすればよい。

この場合においては、クラス固有の鍵が破られた再生回路もしくはメモリカードに対応するクラスを逐次許可クラスリスト CPL から削除していく構成とすればよい。このような構成とすることによっても、再生回路およびメモリカードのクラスごとに配信、移動および再生セッションの実行を禁止することが可能となる。

また、ステップＳ３２４において、移動を目的としてライセンス情報保持部１４４０内の再生情報を取得すると、アクセス制御情報 AC1 を更新し、以降の再生および移動の禁止を記録すると説明したが、当該のデータをライセンス情報保持部１４４０から消去することとしても、同様の効果が得られる。

（実施の形態２）

実施の形態２のデータ配信システムにおいては、実施の形態１のデータ配信システムの構成と異なって、再生回路共通の秘密鍵 Kcom によって復号可能な暗号化を行なわない点を特徴とする。

すなわち、実施の形態２のデータ配信システムは、実施の形態１のデータ配信システムが具備する配信サーバ３０内のライセンスサーバ１０に代えてライセンスサーバ１１を備える点で異なる。また、実施の形態２のデータ配信システムにおける携帯電話機の構成は、図６で説明した携帯電話機１００の構成に代えて携帯電話機１０１の構成が採用される。

図１３を参照して、ライセンスサーバ１１は、ライセンスサーバ１０と比較して、再生回路共通の秘密鍵 Kcom 保持部３２２と、秘密鍵 Kcom による暗号化処理部３２４を具備しない点で異なる。すなわち、ライセンスサーバ１１においては、配信制御部３１５が出力するライセンスキーKc および再生回路制御情報 AC

２は、直接、暗号化処理部３２６に伝達される。その他の回路構成および動作については図４に示すライセンスサーバ１０と同様であるので説明は繰返さない。

以降、ライセンスサーバ１１、認証サーバ１２および配信キャリア２０を合わせて配信サーバ３１と総称することとする。

図１４を参照して、携帯電話機１０１は、実施の形態１で説明した携帯電話機１００の構成と比較して、再生回路共通の秘密鍵Kcomを保持するKcom保持部１５１２と秘密鍵Kcomによる復号処理部１５１４を具備しない点で異なる。

すなわち、携帯電話機１０１においては、配信サーバ３１において秘密鍵Kcomによる暗号化処理が施されていないことに対応して、セッションキーKs４による復号処理を実行する復号処理部１５１０によって直接ライセンスキーKcが得られるため、これを復号処理部１５１０に直接与える構成となる。その他の回路構成および動作については携帯電話機１００の場合と同様であるので説明は繰返さない。

また、実施の形態２に従うデータ配信システムにおいて使用されるメモリカードについては、図７に示すメモリカード１１０と同一の構成であるので説明は繰返さない。

次に、再生回路共通の秘密鍵Kcomによる暗号化を省略することによる、配信、再生および移動の各セッションにおける動作の差異についてフローチャートで説明する。

図１５には、実施の形態２に従うデータ配信システムにおける配信動作を説明するためのフローチャートが示される。図１５においては、図８および図９で示した実施の形態１に従うデータ配信システムにおける配信動作のフローチャートと異なる点について説明する。

図１５を参照して、ステップＳ１３２までの処理は、図８で説明したフローチャートと同一である。図１３で説明したように、ステップＳ１３２で得られるライセンスキーKcおよび再生回路制御情報AC２は、秘密鍵Kcomによる暗号化を施されることなくメモリカード１１０固有の公開暗号鍵KPm（１）によって暗号化されるので、ステップＳ１３４は省略される。以下、ステップＳ１３２に続いて、ステップＳ１３６～Ｓ１４６に代えて、ステップＳ１３６ａ～Ｓ１４６ａ

が実行される。

ステップＳ１３６ａ～Ｓ１４６ａのそれぞれにおいては、ステップＳ１３６～Ｓ１４６において取り扱われるライセンスキーKcおよび再生制御情報AC２が、暗号化した形｛Kc//AC２｝Kcomから、そのままの形であるKc//AC２に代えられて取扱われる点が異なる。その他の暗号化および復号処理については既に図９で説明したのと同様であるので説明は繰返さない。

図１６を参照して、実施の形態２に従うデータ配信システムにおける再生動作においては、図１０に示した実施の形態１に従うデータ配信システムにおける再生動作と比較して、ステップＳ２２２～Ｓ２２６に代えて、ステップＳ２２２ａ～Ｓ２２６ａが実行される点で異なる。

ステップＳ２２２ａ～Ｓ２２６ａのそれぞれにおいては、ステップＳ２２２～Ｓ２２６において取り扱われるライセンスキーKcおよび再生制御情報AC２が、暗号化した形｛Kc//AC２｝Kcomから、そのままの形であるKc//AC２に代えられて取扱われる点が異なる。その他の暗号化および復号処理については既に図１０で説明したのと同様であるので説明は繰返さない。また、その他のステップについては図１０と同様であるので説明は繰返さない。

図１７および図１８を参照して、実施の形態２に従うデータ配信システムにおける移動セッションにおいては、図１１および図１２に示すステップＳ３２６～Ｓ３３６に代えて、ステップＳ３２６ａ～Ｓ３３６ａが実行される点で異なる。

ステップＳ３２６ａ～Ｓ３３６ａのそれぞれにおいては、ステップＳ３２６～Ｓ３３６において取り扱われるライセンスキーKcおよび再生回路制御情報AC２が、暗号化した形｛Kc//AC２｝Kcomから、そのままの形であるKc//AC２に代えられて取扱われる点が異なる。その他の暗号化および復号処理については既に図１１および図１２で説明したのと同様であるので説明は繰返さない。

その他のステップについては図１１および図１２と同様であるので説明は繰返さない。

このような構成とすることによって、再生回路に共通な秘密鍵Kcomを用いない構成としても、実施の形態１に従うデータ配信システムと同様の効果を享受するデータ配信システムを構築することが可能である。

（実施の形態３）

実施の形態１に従うメモリカードにおいては、禁止クラスリスト CRL のデータを TRM 領域内に独自の領域（図７における CRL 保持部１４３０）を設ける構成としていた。実施の形態３に従うメモリカードは、この禁止クラスリスト CRL のデータについてもメモリカード固有の暗号鍵による暗号化を施した上で、TRM 領域外のメモリに暗号化されたコンテンツデータと同様に格納することを特徴とする。

実施の形態３におけるメモリカードをメモリカード１１５とし、メモリカードを識別するための自然数ｉおよびｍを、それぞれｉ＝１およびｍ＝１として説明する。

図１９を参照して、メモリカード１１５は、図７に示す実施の形態１に従うメモリカード１１０と比較して、TRM 領域内に CRL 保持部１４３０を具備しない点で異なる。また、メモリカード１１５は、TRM 領域内に、共通鍵方式における共通鍵であり、メモリカード１１５外から参照することのできないメモリカードごとに固有の共通鍵Ｋ（１）を保持するＫ（１）保持部１４５０と、共通鍵Ｋ（１）による暗号化処理部１４５２および復号処理部１４５４をさらに備える。

図２０を参照して、実施の形態３に従う配信システムにおいては、図４に示した鍵データ等に加えて、メモリカードごとに固有の共通鍵Ｋ（i）が用いられる。共通鍵 Ｋ（i）は、メモリカード内のみで扱われる秘密鍵であり、高速に復号可能な対称鍵である点が、同様にメモリカードごとに固有の非対称な一対の鍵である公開暗号鍵 KPm（i）と秘密復号鍵 Km（i）とは異なる。

再び図１９を参照して、メモリカード１１５においては、禁止クラスリスト CRL は、共通鍵 Ｋ（１）で暗号化されメモリ２４１５に格納される。このように、共通鍵Ｋ（１）で暗号化することで禁止クラスリスト CRL を TRM 領域外に設けられたメモリ２４１５に記録することが可能となる。

また、メモリカード１１０においては、公開暗号鍵 KPm（１）によって暗号化されていたライセンスキーKc を含む再生情報についても、この共通鍵 Ｋ（１）によって暗号化し直すことによって、再生セッションにおける再生開始に至る処理時間の短縮を図ることができる。これは、共通鍵方式における復号が、

公開暗号化方式による復号に対して高速に行なえるためである。また、このような鍵の掛け替えによって、セキュリティー強度が向上する利点も生ずる。

次に、メモリカード１１５を用いたデータ配信システムにおける配信、再生および移動セッションの動作をフローチャートを用いて説明する。

図２１および図２２には、実施の形態３に従うデータ配信システムにおける配信動作を説明フローチャートが示される。実施の形態３に従うデータ配信システムにおける配信セッション時の動作は、コンテンツ配信リクエストの発生から配信サーバ３０におけるライセンスキーKc のデータベースからの取得（ステップＳ１００）からステップＳ１４２までについては、図８および図９に示す場合と同様であるので説明は省略する。

図２２を参照して、ステップＳ１４２において、配信サーバ３０から送信される、暗号化されたライセンスキーを含む再生情報｛｛Kc//AC2｝Kcom//ライセンス ID//コンテンツ ID//AC1｝Km（１）と禁止クラスリスト CRL の更新に用いられる差分データ CRL_dat とが受理される。

配信セッション時のメモリカード１１５においては、図９に示すステップＳ１４４およびＳ１４６に代えて、ステップＳ１４５およびＳ１４７が実行される。

まず、メモリカード１１５においては、暗号化されたライセンスキーを含む再生情報を Km（１）によって復号し、｛Kc//AC2｝Kcom、ライセンス ID、コンテンツ ID および AC1 が受理される（ステップＳ１４５）。

さらに、これらの一部、TRM 領域であるライセンス情報保持部１４４０に記録されない再生情報である｛Kc//AC2｝Kcom は、共通鍵 K（１）によって暗号化処理部１４５２にて暗号化され、TRM 領域外のメモリ２４１５に記録される（ステップＳ１４７）。

ステップＳ１４８においては、実施の形態１の場合と同様に、禁止クラスリストのバージョン更新用情報 CRL_dat に基づいてカード内の禁止クラスリスト CRL が更新される。

更新された禁止クラスリストデータ CRL は、同様に暗号化処理部１４５２で K（１）によって暗号化され、暗号化された禁止クラスリスト｛CRL｝K（１）が TRM 領域外のメモリ２４１５に格納される（ステップＳ１４９）。

その後ステップＳ１５０から配信処理の終了を示すステップＳ１６４までは図９で説明したのと同様であるので説明は繰返さない。

図２３を参照して、再生リクエストが発生するステップＳ２００からコンテンツ再生回路（携帯電話機）の認証を行なうステップＳ２０６までは図１０の場合と同様であるので説明を繰返さない。

メモリカード１１５においては、禁止クラスリスト CRL を暗号化しメモリ２４１５内に格納しているので、禁止クラスリストのチェックに際して、暗号化された禁止クラスリストデータを復号し取出す処置が必要となる。

メモリカード１１５においては、認証データ｛KPp（１）//Cp（１）｝が認証処理によって正当であると確認され、クラス証明書 Cp（１）が承認された場合には（ステップＳ２０６）、メモリに記録された｛CRL｝K（１）を、復号処理部１４５４によって復号して禁止クラスリスト CRL が取得される（ステップＳ２０７）。コントローラ１４２０は、取得された禁止クラスリスト CRL に応じて、コンテンツ再生回路のクラス証明書 Cp（１）が禁止クラスリストに含まれているかどうかの判定を行なう（ステップＳ２０８）。

以下、携帯電話機１１０が禁止クラスリスト CRL の対象外であり、正常に再生が実行される場合には、ステップＳ２１０からステップＳ２２０までが図１０に説明したのと同様に実行される。

メモリカード１１５においては、図１０で説明したメモリカード１１０におけるステップＳ２２２に代えて、ステップＳ２２２ｂが実行される。ステップＳ２２２ｂにおいては、メモリに記録された、ライセンスキーKc および再生制御情報 AC2 が共通鍵 K（１）によって暗号化された｛｛Kc//AC2｝Kcom｝K（１）としてメモリ２４１５に記録されているため、この暗号化データを復号処理部１４５４において共通鍵 K（１）によって復号し｛Kc//AC2｝Kcom を取得するものである。

その後のステップＳ２２４～ステップＳ２４０についても図１０の場合と同様であるので説明は繰返さない。

図２４および図２５には、メモリカード１１５を備えたデータ配信システムにおける移動セッションの動作を説明するフローチャートが示される。

図２４および図２５においては、送信側を携帯電話機１００およびメモリカード１１５とし、受信側を携帯電話機１０２およびメモリカード１１６とする。図１１および図１２の場合と同様に、メモリカード１１６に対応する自然数i＝２，m＝２とする。

図２４のフローチャートを、実施の形態１で説明した図１１のフローチャートと比較すると、メモリカード１１５においては、再生セッションの場合と同様に、メモリカードの KPmc（２）の認証を実行するステップＳ３０８において、認証が有効であった場合には、引続き禁止クラスリストの対象であるか否かを判定する場合に、メモリ２４１５内に格納された禁止クラスリストの暗号化データ{CRL} K（１）を復号する必要が生じる。

具体的には、ステップＳ３０８の認証結果が有効であれば、コントローラ１４２０は、メモリ２４１５から暗号化された禁止クラスリスト {CRL} K（１）を読出して、復号処理部１４５４で復号処理し禁止クラスリスト CRL を取得する（ステップＳ３０９）。

取得した禁止クラスリスト CRL に基づいて、ステップＳ３１０においてメモリカードのクラス証明書が禁止クラスリストの対象となっていないかどうかが判定される。図２４および図２５に示される、ステップＳ３１０以降の処置については図１１および図１２に示したのと同様であるので説明を繰返さない。

このような構成とすることにより、禁止クラスリスト CRL のデータ格納する部分を TRM 内に特別に設ける必要はなくなるので、実施の形態１に従うメモリカードを用いるデータ配信システムが奏する効果に加えて、メモリカードの製造コストが低減されるという利点がある。

また、メモリ２４１５に格納される禁止クラスリストデータ CRL、ライセンスキーKc および再生制御情報 AC2 は、対象鍵である共通鍵K（１）によって新たに暗号化されるので、メモリカードのセキュリティ強度が向上するとともに、データの復号処理を高速に実行できるという利点もさらに生じる。

なお、禁止クラスリストデータ CRL を、TRM 領域外のメモリ領域２４１５内に設けることだけを目的とすれば、共通鍵K（１）を用いずに、メモリカード固有の公開暗号鍵 KPm（１）で禁止クラスリスト CRL を暗号化しメモリ２４１５

内に｛CRL｝Km（１）として格納することによっても実現することが可能である。

すべての実施の形態に従うデータ配信システムにおける配信動作における配信サーバ１０の認証処理において、配信サーバ１０は、メモリカード１１０および携帯電話機（コンテンツ再生回路）１００の認証データ｛KPmc（１）//Cmc（１）｝KPma および｛KPp（１）//Cp（１）｝KPma をともに認証するように説明したが、メモリカードは着脱可能であることから、音楽を再生するコンテンツ再生回路が、必ずしも配信を受けた携帯電話機と同一である必然性はない。また、再生に際してメモリカード内においても再生情報の一部（ライセンスキーKc および再生回路制限情報 AC２）を出力するにあたって、出力先のコンテンツ再生回路の認証データ｛KPp（１）//Cp（１）｝KPma の認証処理を行なっており、配信サーバにおけるコンテンツ再生回路の認証データ｛KPp（１）//Cp（１）｝KPma の認証処理を行なわなくても、セキュリティの低下につながらない。

これらの理由から、配信サーバにおけるコンテンツ再生回路の認証データ｛KPp（１）//Cp（１）｝KPma の認証処理を行なわず、直接の配信先にあたるメモリカード１１０の認証データ｛KPmc（１）//Cmc（１）｝KPma の認証処理のみを行なう構成とすることもできる。

この場合、実施の形態１および２に対する図８と、実施の形態に対応する図２１において、ステップＳ１０４、Ｓ１０６、Ｓ１０８、Ｓ１１０およびＳ１１２において、携帯電話機（コンテンツ再生回路）１００の認証データ｛KPp（１）｝KPma、公開暗号鍵 KPp（１）クラス証明書 Cp（１）に対する処理をすべて省略すれば実現することができる。

また、ステップＳ１０４において、コンテンツＩＤ、メモリカード１１０の認証データ｛KPmc（１）//Cmc（１）｝KPma およびライセンス購入条件 AC を配信サーバに送信し、ステップＳ１０６において、配信サーバ１０はメモリカード１１０の認証データ｛KPmc（１）//Cmc（１）｝KPma およびライセンス購入条件 AC を受信し、ステップＳ１０８において、認証鍵 KPma によって、認証データ｛KPmc（１）//Cmc（１）｝KPma を復号し、さらに、ステップＳ１１０において、復号結果に基づいて認証処理を行ない、正当なメモリカードからの認証デ

ータである場合においては、クラス証明書 Cmc（１）を承認する。一方、認証データが正当でない場合においては、配信処理は終了する。

ステップＳ１１２において、承認したクラス証明書 Cmc（１）が CRL データベース３０６からの禁止クラスリスト CRL にリストアップされたクラス証明書に含まれるかどうかを判断する。禁止クラスリスト CRL に含まれなければ配信処理は続けられ、含まれた場合には配信処理は終了する。以降のステップにおける処理については、このような認証処理を行なった場合においても、実施の形態１および２で説明したのと同様に実行することができる。

また、再生動作および移動動作においては、このような認証処理を行なうこととしても、実施の形態１および２ですでに説明したのと同様のフローに従って処理することができる。

さらに、実施の形態１および２に用いたメモリカード１１０において、十分な TRM 領域が確保できる場合において、ライセンス保持部１４４０に、復号して平文となったすべての再生情報（ライセンスキーKc、再生回路制御情報 AC２、ライセンス ID、コンテンツ ID およびアクセス制限情報 AC１）を保持しても、セキュリティ上の問題はなく、メモリカード１１０の処理が変更になるのみで、同様な効果を得ることができる。

以下に、平文となったすべての再生情報をライセンス保持部１４４０に保持するケースに対応するために、実施の形態１および２で説明した、配信処理、再生処理および移動処理の動作フローに変更を加える必要がある個所について説明する。

このようなケースに対応するためには、実施の形態１に従う配信処理においては、図９におけるステップＳ１４４を省いて、ステップＳ１４６において、復号して得られたすべての再生情報（ライセンスキーKc、再生回路制御情報 AC２、ライセンス ID、コンテンツ ID およびアクセス制限情報 AC１）を受理し、ステップＳ１５０において、受理したすべての再生情報をライセンス情報保持部１４４０に記録すればよい。

実施の形態１に従う再生処理においては、図１０におけるステップＳ２２０において、ライセンス情報保持部に記録されている再生リクエスト曲の｛Kc//AC

2）Kcom を取得するように変更する。再生処理における他のステップにおいては処理の変更は必要ない。

実施の形態１に従う移動処理においては、図１１におけるステップＳ３２４において、ライセンス情報保持部１４４０に保持されたすべての再生情報を取得して、ステップＳ３２６の処理を省略すればよい。その他のステップに対する変更は必要ない。

同様に、実施の形態２に従う配信処理においては、図１５中のステップＳ１４４ａを省略して、ステップＳ１４６ａにおいて、復号して得られたすべての再生情報（ライセンスキーKc、再生回路制御情報 AC２、ライセンス ID、コンテンツ ID およびアクセス制限情報 AC１）を受理し、ステップＳ１５０において、受理したすべての再生情報をライセンス情報保持部１４４０に記録すればよい。

また、実施の形態２に従う再生処理においては、図１６中のステップＳ２２２ａにおける処理を、ライセンス情報保持部１４４０に記録されている再生リクエスト曲のライセンスキーKc および再生回路制限情報 AC２を取得するように変更するのみでよく、他のステップにおける動作の変更は必要ない。

実施の形態２に従う移動処理においては、図１７中のステップＳ３２４において、ライセンス情報保持部１４４０に保持されたすべての再生情報を取得して、ステップＳ３２６ａの処理を省略することによって対応できる。

以上に説明した動作フローの変更を行うことによって、平文となったすべての再生情報をライセンス保持部１４４０に保持するケースにおいても、実施の形態１および２と同様の、配信処理、再生処理および移動処理を実行することができる。

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

産業上の利用可能性

この発明によるデータ配信システムおよび記録装置は、携帯電話機のような移動通信端末を利用したデータ配信に用いることができる。

請求の範囲

1．データ配信システムであって、

複数の端末（１００，１０１）と、

暗号化コンテンツデータ（｛Data｝Kc）と、前記暗号化コンテンツデータを復号して平文のコンテンツデータ（Data）を得るための復号鍵であるライセンスキー（Kc）とを前記複数の端末に配信するためのコンテンツ供給装置（１０，１１）とを備え、

各前記端末は、

外部との間でデータを授受するための第１のインタフェース部（１１０２）と、

少なくとも前記ライセンスキーを受けて記録する配信データ解読部（１１０，１１５）とを含み、

前記配信データ解読部は、

認証鍵（KPma）によって復号することで認証可能な状態に暗号化された、前記配信データ解読部に対応して定められる第１のクラス証明データ（Cmc(m)）を保持し、前記ライセンスキーを受信する場合に、前記第１のインタフェース部を介して出力する第１の認証データ保持部（１４００）と、

前記暗号化コンテンツデータおよび前記ライセンスキーを記録するための第１の記憶部（１４１５，１４４０）とを有し、

前記コンテンツ供給装置は、

外部との間でデータを授受するための第２のインタフェース部（３５０）と、

前記認証鍵によって復号することで正当性を証明できる状態に暗号化された前記第１のクラス証明データを前記第２のインタフェース部から受け取って、前記認証鍵によって復号して前記正当性を確認するための第１の認証処理部（３１２）と、

前記配信の禁止対象となされる前記第１のクラス証明データをリストアップした禁止クラスリスト（CRL）を保持するための禁止クラスリスト保持部（３０６）と、

前記第１の認証処理部において得られた前記第１のクラス証明データが禁止ク

ラスリスト保持部に保持される前記禁止クラスリストに含まれる場合には、前記少なくとも前記コンテンツキーの配信動作を中止する配信制御部（３１５）とを含む、データ配信システム。

２．　前記配信データ解読部（１１０，１１５）は、前記端末に着脱可能な記録装置であり、

前記第１のクラス証明データ（Cmc(m)）は、前記記録装置の種類ごとに対応して予め定められる、請求の範囲第１項に記載のデータ配信システム。

３．　前記配信データ解読部（１１０，１１５）は、

前記禁止クラスリスト（CRL）を保持するための第２の記憶部（１４３０，２１４５）と、

前記配信動作が指示されるのに応じて、前記第２の記憶部に保持される前記禁止クラスリストの更新を特定できる更新情報（CRL_ver）を抽出して、前記第２のインタフェース部（１１０２）を介して前記コンテンツ供給装置（１０，１１）に対して出力する制御部（１４２０）とをさらに有し、

前記コンテンツ供給装置は、前記更新情報を前記第２のインタフェース部（３５０）を介して前記配信制御部（３１５）へ与え、

前記配信制御部は、前記更新情報に基づいて、前記第２の記憶部に保持される前記禁止クラスリストを新しい禁止クラスリストに更新するための更新データ（CRL_dat）を作成し、前記第２のインタフェース部を介して前記更新データを出力し、

前記制御部は、前記第１のインタフェース部を介して受けた前記更新データに基づいて、前記第２の記憶部に保持される前記禁止クラスリストの内容を更新する、請求の範囲第１項に記載のデータ配信システム。

４．　前記配信データ解読部（１１０，１１５）は、

前記認証鍵（KPma）による復号を行なって前記正当性を確認するための第２の認証処理部（１４０８）をさらに有し、

前記配信データ解読部は、外部から指示される、前記暗号化コンテンツデータ（{Data} Kc）および前記ライセンスキー（Kc）の少なくとも一方を他の配信データ解読部（１１２，１１６）に移動させる移動動作において、前記他の配信

データ解読部に対応する、前記認証鍵によって復号することで前記正当性が証明できる状態に暗号化された、前記第１のクラス証明データ（Cmc(m)）を取得し、

前記制御部（１４２０）は、前記第２の認証処理部において得られた前記他の配信データ解読部に対応する前記第１のクラス証明データが前記第２の記憶部（１４３０，２１４５）に保持される前記禁止クラスリスト（CRL）に含まれる場合には、少なくとも前記ライセンスキーの前記移動動作を中止する、請求の範囲第３項に記載のデータ配信システム。

５．　各前記端末（１００，１０１）は、コンテンツ再生部（１５５０）をさらに含み、

前記コンテンツ再生部は、

前記配信データ解読部（１１０，１１５）から前記ライセンスキー（Kc）と前記暗号化コンテンツデータ（｛Data｝Kc）とを受けて、前記ライセンスキーにより前記暗号化コンテンツデータを復号して再生するコンテンツデータ再生部（１５１６，１５１８）と、

前記認証鍵（KPma）によって復号することで前記正当性が証明できる状態に暗号化された、前記コンテンツ再生部に対応して予め定められる、第２のクラス証明データ（Cp(n)）を保持する第２の認証データ保持部（１５００）とを有し、

前記第１の認証処理部（３１２）は、暗号化された前記第２のクラス証明データを、前記第２のインタフェース部（３５０）から受け取って復号処理を行ない、

前記禁止クラスリスト保持部（３０６）に保持された前記禁止クラスリスト（CRL）は、禁止対象とされる前記第２のクラス証明データをさらにリストアップし、

前記配信動作において、各前記端末（１００，１０１）は、暗号化された前記第２のクラス証明データを前記第１のインタフェース部（１１０２）を介して前記第２のインタフェース部に対して出力し、

前記配信制御部（３１５）は、前記第２のインタフェース部を介して入力され、前記第１の認証処理部によって復号された前記第２のクラス証明書データが、前記禁止クラスリスト保持部に保持される前記禁止クラスリストに含まれる場合には、前記配信動作を中止する、請求の範囲第１項に記載のデータ配信システム。

6．　各前記端末は、コンテンツ再生部（１５５０）をさらに備え、

前記コンテンツ再生部は、

前記配信データ解読部（１１０，１１５）から前記ライセンスキー（Kc）と前記暗号化コンテンツデータ（｛Data｝Kc）とを受けて、前記ライセンスキーにより前記暗号化コンテンツデータを復号して再生するコンテンツデータ再生部（１５１６，１５１８）と、

前記認証鍵（KPma）によって復号することで前記正当性が証明可能な状態に暗号化された、前記コンテンツ再生部に対応して予め定められる第２のクラス証明データ（Cp(n)）を保持する第２の認証データ保持部（１５００）とを有し、

前記配信データ解読部は、

前記認証鍵による復号を行って前記正当性を確認するための第２の認証処理部（１４０８）をさらに有し、

前記第２の記憶部（１４３０，２１４５）に保持された前記禁止クラスリスト（CRL）は、禁止対象となされる前記第２のクラス証明データをさらにリストアップし、

前記配信データ解読部は、外部から指示される、前記暗号化コンテンツデータを前記コンテンツ再生部によって再生する再生動作において、前記第１の記憶部（１４１５，１４４０）から前記暗号化コンテンツデータおよびライセンスキーを出力し、

前記配信データ解読部は、前記再生動作において、前記コンテンツ再生部に対応する、前記認証鍵によって復号することで前記正当性が証明できる状態に暗号化された前記第２のクラス証明データを取得し、

前記制御部（１４２０）は、前記再生動作時において、前記第２の認証処理部によって得られた前記第２のクラス証明データが前記第２の記憶部に保持される前記禁止クラスリストに含まれる場合には、前記再生動作を中止する、請求の範囲第３項に記載のデータ配信システム。

7．　前記第１のインタフェース部（３５０）と前記第２のインタフェース部（１１０２）とは、携帯電話網によって接続され、

前記配信制御部（３１５）は、前記配信動作時において、前記第１のクラス証

明データ（Cmc(m)）に基づいて前記配信データ解読部（１１０，１１５）の認証を行なう、請求の範囲第１項に記載のデータ配信システム。

８．　各前記端末（１００，１０１）は、前記携帯電話網に接続して通話を行なう通信処理部をさらに含む、請求の範囲第７項に記載のデータ配信システム。

９．　前記コンテンツ再生部（１５５０）は、前記端末（１００，１０１）に着脱可能な構成である、請求の範囲第５項に記載のデータ配信システム。

１０．　前記第１の記憶部（１４１５，１４４０）は、半導体メモリであり、

前記記録装置は、メモリカードである、請求の範囲第２項に記載のデータ配信システム。

１１．　記録装置であって、

データ（Kc）を記録するための第１の記憶部（１４１５，１４４０）と、

インタフェース部（１２０２）を介して入力される、認証鍵(KPma)によって復号することで認証可能な状態に暗号化された第１のクラス証明データ（Cp(n)）を受けて、前記認証鍵(KPma)による復号を行なって正当性を確認するための認証処理部（１４０８）と、

前記データの出力を禁止する対象となされる第１のクラス証明データをリストアップした禁止クラスリスト（CRL）を保持するための第２の記憶部（１４３０，２１４５）と、

外部からの前記データの出力指示に応じて、前記インタフェース部を介して前記データの出力を指示する制御部（１４２０）とを備え、

前記制御部は、前記出力指示とともに外部から前記インタフェース部を介して入力される、前記暗号化がなされた第１のクラス証明データを前記認証処理部で復号して得られる前記第１のクラス証明データが前記禁止クラスリストに含まれる場合において、前記データの出力を中止する、記録装置。

１２．　前記認証鍵（KPma）によって復号可能な状態に暗号化された、前記記録装置に対応して定められる第２のクラス証明データ（Cmc(m)）を保持する認証データ保持部（１４００）をさらに備え、

前記認証データ保持部は、外部からの前記データ（Kc）の入力指示に応じて、前記認証データ保持部に保持される、前記認証鍵によって復号することで正当性

を証明できる状態に暗号化された前記第２のクラス証明データを前記インタフェース部（１２０２）を介して出力する、請求の範囲第１１項に記載の記録装置。

１３．　前記入力指示に応じて、前記インタフェース部（１２０２）を介して前記データ（Kc）の入力を受けて、前記第１の記憶部（１４１５，１４４０）に記録する記録動作において、

前記制御部（１４２０）は、前記記録動作が指示されるのに応じて、前記第２の記憶部（１４３０，２１４５）に保持される前記禁止クラスリスト（CRL）の更新を特定できる更新情報（CRL_ver）を抽出し、前記更新情報を前記インタフェース部を介して外部に出力し、

前記制御部は、前記更新情報に基づいて生成される、前記禁止クラスリストを新しい禁止クラスリストに更新するための更新データ（CRL_dat）を、外部から前記インタフェース部を介して受けて、前記更新データに基づいて前記禁止クラスリストの内容を更新する、請求の範囲第１２項に記載の記録装置。

１４．　前記第１の記憶部（１４１５，１４４０）は、半導体メモリであり、

前記記録装置は、メモリカードである、請求の範囲第１１項に記載の記録装置。

１５．データ配信システムであって、

暗号化コンテンツデータ（｛Data｝Kc）と、前記暗号化コンテンツデータを復号して平文のコンテンツデータ（Data）を得るための復号鍵であるライセンスキー（Kc）とを配信するためのコンテンツ供給装置（１０，１１）と、

前記コンテンツ供給装置（１０，１１）からの前記配信を受ける複数の端末（１００，１０１）とを備え、

前記コンテンツ供給装置は、

外部との間でデータを授受するための第１のインタフェース部（３５０）と、

認証鍵(KPma)によって復号することで認証可能な状態に暗号化された、第１のクラス証明データ（Cmc(m)）および第１の公開暗号鍵（KPmc(m)）を、前記第１のインタフェース部から受けて前記認証鍵による復号を行なって正当性を確認するための第１の認証処理部（３１２）と、

前記ライセンスキーの配信の禁止対象となされる前記第１のクラス証明データをリストアップした禁止クラスリスト（CRL）を保持する禁止クラスリスト保持

部（３５０）と、

前記第１の認証処理部において得られた前記第１のクラス証明データが前記禁止クラスリスト保持部に保持される前記禁止クラスリストに含まれる場合には、少なくとも前記ライセンスキーを含む第１の再生情報の配信動作を中止する配信制御部（３１５）と、

前記配信ごとに更新される第１の共通鍵（Ks1）を生成する第１のセッションキー発生部（３１６）と、

前記第１の公開暗号鍵によって前記第１の共通鍵を暗号化して前記第１のインタフェース部に与えるためのセッションキー暗号化部（３１８）と、

前記第１の共通鍵によって暗号化されて前記第１のインタフェース部を介して返信される、第２の公開暗号鍵（KPm(i)）および第２の共通鍵（Ks2）を復号抽出するためのセッションキー復号部（３２０）と、

前記第１の再生情報を、前記セッションキー復号部により復号された前記第２の公開暗号鍵によって暗号化する第１のライセンスデータ暗号化処理部（３２６）と、

前記第１のライセンスデータ暗号化処理部の出力を、前記セッションキー復号部により復号された前記の第２の共通鍵によってさらに暗号化して、前記第１のインタフェース部に与え配信するための第２のライセンスデータ暗号化処理部（３２８）とを含み、

各前記端末は、

外部との間でデータを授受するための第２のインタフェース部（１１０２）と、

前記暗号化コンテンツデータを受けて記録する配信データ解読部（１１０，１１５）とを含み、

第１のクラス証明データ（Cmc(m)）および第１の公開暗号鍵（KPmc(m)）は、前記配信データ解読部に対応して定められ、

前記配信データ解読部は、

前記認証鍵によって復号することで前記正当性を証明できる状態に暗号化された、前記第１のクラス証明データおよび前記第１の公開暗号鍵を保持し、前記第１の再生情報を受信する場合に出力する第１の認証データ保持部（１４００）と、

前記第１の公開暗号鍵によって暗号化されたデータを復号化するための第１の秘密復号鍵（Kmc(m)）を保持する第１の鍵保持部（１４０２）と、

前記第１の公開暗号鍵によって暗号化された前記第１の共通鍵を受けて、復号処理するための第１の復号処理部（１４０４）と、

前記第２の公開暗号鍵を保持する第２の鍵保持部（１４１６）と、

前記暗号化コンテンツデータの通信ごとに更新される前記第２の共通鍵を生成する第２のセッションキー発生部（１４１８）と、

前記第２の共通鍵および前記第２の公開暗号鍵を前記第１の共通鍵によって暗号化し、前記第２のインタフェース部に出力するための第１の暗号化処理部（１４０６）と、

前記第２のライセンスデータ暗号化処理部から、暗号化された前記第１の再生情報を受けて、前記第２の共通鍵によって復号するための第２の復号処理部（１４１２）と、

前記第２の公開暗号鍵によって暗号化されたデータを復号するための第２の秘密復号鍵（Km(i)）を保持する第３の鍵保持部（１４２１）と、

前記第２の秘密復号鍵による復号処理を実行するための第３の復号処理部（１４２２）と

前記第１の再生情報および前記暗号化コンテンツデータを記録するための第１の記憶部（１４１５，１４４０）とを有する、データ配信システム。

１６．前記配信データ解読部（１１０，１１５）は、前記端末（１００，１０１）に着脱可能な記録装置であり、

前記第１の秘密復号鍵（Kmc(m)）は、前記記録装置の種類ごとに異なる、請求の範囲第１５項に記載のデータ配信システム。

１７．　前記第２および前記第３の復号処理部（１４１２，１４２２）は、前記コンテンツ供給装置（１０，１１）において前記第２の公開暗号鍵（KPm(i)）で暗号化され、さらに前記第２の共通鍵（Ks2）で暗号化されて、前記第１の再生情報とともに配信される第２の再生情報（AC1）を前記第２のインタフェース部（１１０２）を介して受け、前記第２の共通鍵および前記第２の秘密復号鍵（Km(i)）によって復号し、

前記第１の記憶部（１４１５，１４４０）は、前記第２の再生情報をさらに記録する、請求の範囲第１５項に記載のデータ配信システム。

１８．　前記配信データ解読部（１１０，１１５）は、

前記禁止クラスリスト（CRL）を保持するための第２の記憶部（１４３０，２４１５）と、

前記暗号化コンテンツデータ（｛Data｝Kc）の配信動作が指示されるのに応じて、前記第２の記憶部に保持される前記禁止クラスリストの更新を特定できる更新情報（CRL_ver）を生成する制御部（１４２０）とをさらに有し、

前記第１の暗号化処理部（１４０６）は、さらに、前記更新情報を前記第１の共通鍵（Ks1）によって暗号化して前記第２のインタフェース部（１１０２）に出力し、

前記配信制御部（３１５）は、前記セッションキー復号部（３２０）によって復号された前記更新情報に基づいて、前記第２の記憶部に保持される前記禁止クラスリストを新しい禁止クラスリストに更新するための更新データ（CRL_dat）を生成し、

前記コンテンツ供給装置は、前記更新データを前記第２の共通鍵（Ks2）で暗号化して前記第１のインタフェース部（３５０）より出力し、

前記第２の復号処理部（１４１２）は、前記第２のインタフェース部を介して受ける暗号化された前記更新データを前記第２の共通鍵によって復号し、

前記制御部（１４２０）は、前記更新データに基づいて、前記第２の記憶部に保持される前記禁止クラスリストの内容を更新する、請求の範囲第１５項に記載のデータ配信システム。

１９．　前記第２の記憶部（１４３０，２１４５）は、第三者に読出不可能なセキュリティー領域（TRM）内に配置される、請求の範囲第１８項に記載のデータ配信システム。

２０．　前記第２のセッションキー発生部（１４１８）は、外部から指示される前記コンテンツデータの再生動作においては、前記指示に応答して第３の共通鍵（Ks3）を生成し、

前記第１の記憶部（１４１５，１４４０）は、前記制御部（１４２０）に制御

されて、前記再生動作の指示に応じて、記録した前記暗号化コンテンツデータ（{Data} Kc）および前記第１の再生情報を出力し、

前記第３の復号処理部（１４２２）は、前記再生動作において、前記第１の記憶部から出力された前記第１の再生情報が暗号化されている場合に、復号を行なって前記第１の再生情報を抽出し、

前記第１の暗号化処理部（１４０６）は、前記再生動作においては、前記第３の復号処理部および前記第１の記憶部のいずれか一方から前記第１の再生情報を受けて、第４の共通鍵（Ks4）に基づいて暗号化し、

前記配信データ解読部（１１０，１１５）は、前記第４の共通鍵によって暗号化された前記第１の再生情報および前記暗号化コンテンツデータを出力し、

各前記端末（１００，１０１）は、コンテンツ再生部（１５５０）をさらに含み、

前記コンテンツ再生部は、

前記配信データ解読部からの、前記第４の共通鍵によって暗号化された前記第１の再生情報を復号して、前記第１の再生情報を抽出する第４の復号処理部（１５１０）と、

前記暗号化コンテンツデータを、前記第４の復号処理部からの出力である前記第１の再生情報に含まれる前記ライセンスキー（Kc）により復号して再生するコンテンツデータ再生部（１５１６，１５１８）と、

前記認証鍵（KPma）によって復号することで正当性を証明できる状態に暗号化された、前記コンテンツ再生部に対応して予め定められる、第２のクラス証明データ（Cp（n））および第３の公開暗号鍵（KPp(n)）を保持し、前記再生動作に応じて前記配信データ解読部（１１０，１１５）に対して出力する第２の認証データ保持部（１５００）と、

前記第３の公開暗号鍵によって暗号化されたデータを復号化するための第３の秘密復号鍵（Kp(n)）を保持する第４の鍵保持部（１５０２）と、

前記第３の公開暗号鍵によって暗号化されて返信されるデータを前記第３の秘密復号鍵によって復号して前記第３の共通鍵を得るための第５の復号処理部（１５０４）と、

前記再生動作ごとに更新される前記第４の共通鍵を生成する第３のセッションキー発生部（１５０８）と、

前記第５の復号処理部から受ける前記第３の共通鍵によって、前記第４の共通鍵を暗号化して前記配信データ解読部に対して出力する第２の暗号化処理部（１５０６）とを有し、

前記配信データ解読部（１１０，１１５）は、

前記認証鍵によって復号することで正当性を証明できる状態に暗号化された、前記第２のクラス証明データおよび前記第３の公開暗号鍵を、前記認証鍵(KPma)によって復号して前記正当性を確認するための第２の認証処理部（１４０８）と、

前記制御部（１４２０）に制御されて、前記第２の認証処理部から受ける前記第３の公開暗号鍵によって前記第２の共通鍵を暗号化して、対応する前記コンテンツ再生部（１５５０）に対して出力するための第３の暗号化処理部（１４１０）とをさらに有し、

前記禁止クラスリスト（CRL）は、禁止対象とされる前記第２のクラス証明データをさらにリストアップし、

前記制御部（１４２０）は、前記再生動作において、前記第２の認証処理部において得られた前記第２のクラス証明データが前記第２の記憶部に保持される前記禁止クラスリストに含まれている場合には、前記再生動作を中止する、請求の範囲第１８項に記載のデータ配信システム。

２１．　前記第２および前記第３の復号処理部（１４１２，１４２２）は、前記コンテンツ供給装置（１０，１１）において前記第２の公開暗号鍵（KPm(i)）で暗号化され、さらに前記第２の共通鍵（Ks2）で暗号化されて、前記第１の再生情報（AC2）とともに配信される第２の再生情報（AC1）を前記第２のインタフェース部（１１０２）を介して受けて、前記第２の共通鍵および前記第２の秘密復号鍵（Km(i)）によって復号し、

前記第１の記憶部（１４４０）は、配信データ解読部（１１０，１１５）は、復号された前記第２の再生情報をさらに記録し、

前記制御部（１４２０）は、前記再生動作において、前記第１の記憶部に記録

された前記第２の再生情報に基づいて前記第１の再生情報の出力可否を判断する、請求の範囲第２０項記載のデータ配信システム。

２２．　前記第２の認証処理部（１４０８）は、外部から指示される、前記配信データ解読部（１１０，１１５）から他の配信データ解読部（１１２，１１６）に対して少なくとも前記第１の再生情報を含むデータを移転するための移動動作に応じて、前記認証鍵によって復号することで正当性を証明できる状態に暗号化された、前記他の配信データ解読部に対応する、前記第１のクラス証明データ（Cmc(m)）および前記第１の公開暗号鍵（KPmc(m)）を前記第２のインタフェース部から受け取って、前記認証鍵(KPma)によって復号して前記正当性を確認し、

前記配信データ解読部および前記他の配信データ解読部にそれぞれ対応する複数の前記第２のセッションキー発生部（１４１８）は、前記移動動作に応じて、前記第３および第２の共通鍵（Ks3，Ks2）をそれぞれ生成し、

前記第３の暗号化処理部（１４１０）は、前記移動動作時において、前記他の配信データ解読部に対応する前記第１の公開暗号鍵によって前記配信データ解読部（１１２，１１６）に対応する前記第３の共通鍵を暗号化して、前記他の配信データ解読部に対して出力し、

前記第２の復号処理部（１４１２）は、前記移動動作時において、前記第３の共通鍵によって暗号化されて前記他の配信データ解読部から返信されるデータを復号して、前記他の配信データ解読部（１１２，１１６）で生成された前記第２の共通鍵および前記他の配信データ解読部に対応する前記第２の公開暗号鍵を取得し、

前記配信データ解読部は、

前記移動動作において、前記第１の記憶部（１４４０）から出力される前記第１の再生情報を、前記他の配信データ解読部に対応する前記第２の公開暗号鍵によってさらに暗号化するための第４の暗号化処理部（１４２４）と、

前記移動動作時において、前記第４の暗号化処理部（１４２４）の出力および前記第２の復号処理部（１４１２）によって取得された前記第２の共通鍵を前記第１の暗号化処理部（１４０６）に伝達するためのデータスイッチ（１４４２，

１４４６）とをさらに有し、

前記第１の暗号化処理部（１４０６）は、前記移動動作時において、前記第４の暗号化処理部（１４２４）の出力を、前記他の配信データ解読部（１１２，１１６）で生成された前記第２の共通鍵によってさらに暗号化して、前記他の配信データ解読部に対して出力し、

前記制御部（１４２０）は、前記移動動作において、前記第２の認証処理部において得られた前記他の配信データ解読部に対応する前記第１のクラス証明データが前記第２の記憶部に保持される前記禁止クラスリストに含まれている場合には、前記移動動作を中止する、請求の範囲第２０項に記載のデータ配信システム。

２３．　前記制御部（１４２０）は、前記移動動作において、前記他の配信データ解読部（１１２，１１６）に対応する前記第１のクラス証明データ（Cmc(m)）に基づいて、前記他の配信データ解読部の認証を行なう、請求の範囲第２２項に記載のデータ配信システム。

２４．　前記第４の暗号化処理部（１４２４）は、前記禁止クラスリストのデータを前記第２の公開暗号鍵（KPm(i)）で暗号化し、

前記第２の記憶部（２４１５）は、第三者に読出不可能なセキュリティー領域（TRM）外に設けられて、前記第４の暗号化処理部によって暗号化された前記禁止クラスリストを保持する、請求の範囲第２２項に記載のデータ配信システム。

２５．　前記第２および前記第３の復号処理部（１４１２，１４２２）は、前記コンテンツ供給装置（１０，１１）において前記第２の公開暗号鍵（KPm(i)）で暗号化され、さらに前記第２の共通鍵（Ks2）で暗号化されて、前記第１の再生情報（AC2）とともに配信される第２の再生情報（AC1）を前記第２のインタフェース部（１１０２）を介して受け、前記第２の共通鍵および前記第２の秘密復号鍵（Km(i)）によって復号し、

前記第１の記憶部（１４４０）は、復号された前記第２の再生情報をさらに記録し、

前記制御部（１４２０）は、前記移動動作時において、前記第１の記憶部に記録された第２の再生情報に基づいて前記移動動作の実行可否を判断するとともに、前記暗号化コンテンツデータ（｛Data｝Kc）を前記他の配信データ解読部（１

１２，１１６）に出力することを指示した場合には前記第２の再生情報を更新する、請求の範囲第２０項に記載のデータ配信システム。

２６．　前記制御部（１４２０）は、前記再生動作において、前記第２のクラス証明データ（Cp(n)）に基づいて前記コンテンツ再生部（１５５０）の認証を行なう、請求の範囲第２０項に記載のデータ配信システム。

２７．　前記配信データ解読部（１１５）は、

前記記録装置ごとに異なる秘密鍵（K(i)）を保持する第５の鍵保持部（１４５０）と、

前記第２の復号処理部（１４１２）の出力を前記第３の復号処理部（１４２２）において前記第２の秘密復号鍵（Km(i)）によって復号して得られるデータを前記秘密鍵で暗号化するための第５の暗号化処理部（１４５２）と、

前記秘密鍵で暗号化されたデータを復号するための第６の復号処理部（１４５４）とをさらに有し、

前記第１の記憶部（１４１５）は、前記第５の暗号化処理部によって暗号化されたデータを記録し、

前記第５の暗号化処理部は、前記禁止クラスリスト（CRL）のデータを前記秘密鍵で暗号化し、

前記第２の記憶部（２４１５）は、第三者に読出不可能なセキュリティー領域（TRM）外に設けられて、前記第５の暗号化処理部によって暗号化された前記禁止クラスリストを保持する、請求の範囲第１８項に記載のデータ配信システム。

２８．前記コンテンツ供給装置（１０，１１）は、

前記コンテンツ再生部（１５５０）にて再生可能な共通秘密鍵（Kcom）を保持する第６の鍵保持部（３２２）と、

前記第１の再生情報を前記共通秘密鍵によって暗号化し、前記第１のライセンスデータ暗号化処理部（３２６）に対して出力する第３のライセンスデータ暗号化部（３２４）をさらに含み、

前記コンテンツ再生部（１５５０）は、

前記共通秘密鍵を保持する第７の鍵保持部（１５１２）と、

前記第４の復号処理部（１５１０）の出力を受けて、前記第７の鍵保持部に保

持された前記共通秘密鍵によって前記第１の再生情報を復号し、前記ライセンスキー（Kc）を抽出して前記コンテンツデータ再生部（１５１６，１５１８）に対して出力するための第７の復号処理部（１５１４）をさらに有する、請求項２０記載のデータ配信システム。

２９．　前記コンテンツ供給装置（１０）は、

前記コンテンツデータ再生部にて再生可能な第４の公開暗号鍵を保持する第７の鍵保持部と、

前記ライセンスキーを少なくとも含む前記第１の再生情報を前記第４の公開暗号鍵にて暗号化し、前記第１のライセンスデータ暗号化処理部に対して出力する第３のライセンスデータ暗号化部をさらに含み、

前記コンテンツ再生部（１５５０）は、

前記第４の公開暗号鍵によって暗号化された前記第１の再生情報を復号できる第４の秘密復号鍵を保持する第７の鍵保持部と、

前記第４の復号処理部（１５１０）の出力を受けて、前記第７の鍵保持部に保持された前記第４の秘密復号鍵によって前記第１の再生情報を復号し、前記ライセンスキーを抽出して前記コンテンツ再生部に対して出力する第７の復号処理部をさらに有する、請求の範囲第２０項に記載のデータ配信システム。

３０．データ配信システムであって、

暗号化コンテンツデータ（｛Data｝Kc）と、前記暗号化コンテンツデータを復号して平文のコンテンツデータ（Data）を得るための復号鍵であるライセンスキー（Kc）とを配信するためのコンテンツ供給装置（１０，１１）と、

前記コンテンツ供給装置（１０，１１）からの前記配信を受ける複数の端末（１００，１０１）とを備え、

前記コンテンツ供給装置（１０，１１）は、

外部との間でデータを授受するための第１のインタフェース部（３５０）と、

認証鍵(KPma)によって復号することで認証可能な状態に暗号化されたクラス証明データ（Cmc(m)）を、前記第１のインタフェース部から受け取って前記認証鍵によって復号処理するための認証処理部（３１２）と、

前記暗号化コンテンツデータの配信の許可対象である前記クラス証明データを

リストアップした許可クラスリストを保持する許可クラスリスト保持部と、

前記認証処理部において得られた前記クラス証明データが前記許可クラスリスト保持部に保持される前記許可クラスリストに含まれる場合には、少なくとも前記ライセンスキーの配信動作を実行する配信制御部（３１５）とを含み

各前記端末（１００，１０１）は、

外部との間でデータを授受するための第２のインタフェース部（１１０２）と、

少なくとも前記ライセンスキーを受けて記録する配信データ解読部（１１０，１１５）とを含み、

前記クラス証明データは、前記配信データ解読部に対応して定められ、

前記配信データ解読部は、

前記認証鍵によって復号することで正当性を証明できる状態に暗号化された前記クラス証明データを保持し、前記ライセンスキーを受信する場合に、前記第２のインタフェース部を介して出力する認証データ保持部（１４００）と、

前記暗号化コンテンツデータおよび前記ライセンスキーを記録するための第１の記憶部（１４１５，１４４０）とを有する、データ配信システム。

３１．　前記配信データ解読部（１１０，１１５）は、前記端末（１００，１０１）に着脱可能な記録装置であり、

前記クラス証明データ（Cmc(m)）は、前記記録装置の種類ごとに対応して予め定められ、

前記配信データ解読部（１１０，１１５）は、

前記許可クラスリストを保持するための第２の記憶部と、

前記配信動作が指示されるのに応じて、前記第２の記憶部に保持される前記許可リストの更新を特定できる更新情報を生成する制御部（１４２０）とをさらに有し、

前記制御部は、前記更新情報を前記第２のインタフェース部（１１０２）を介して前記コンテンツ供給装置（１０，１１）に対して出力し、

前記コンテンツ供給装置は、前記第１のインタフェース部（３５０）を介して前記更新情報を受けて、前記配信制御部（３１５）へ与え、

前記配信制御部は、前記更新情報に基づいて、前記許可クラスリストを新しい

許可クラスリストに更新するための更新データを作成して、前記第１のインタフェース部を介して前記更新データを出力し、

前記制御部は、前記第２のインタフェース部（１１０２）を介して前記更新データを受けて、前記更新データに基づいて、前記第２の記憶部に保持される前記許可クラスリストの内容を更新する、請求の範囲第３０項に記載のデータ配信システム。

３２．　暗号化コンテンツデータ（｛Data｝Kc）と、前記暗号化コンテンツデータを復号して平文のコンテンツデータ（Data）を得るための復号鍵であるライセンスキー（Kc）とを受けて記録するための記録装置であって、

外部との間でデータを授受するためのインタフェース部（１２０２）と、

認証鍵(KPma)によって復号することで認証可能な状態に暗号化された、前記記録装置に対応して定められる、第１のクラス証明データ（Cmc(m)）および第１の公開暗号鍵（KPmc(m)）を保持し、前記暗号化コンテンツデータを受信する場合において前記インタフェース部を介して外部に出力する認証データ保持部（１４００）と、

前記第１の公開暗号鍵によって暗号化されたデータを復号化するための第１の秘密復号鍵（Kmc(m)）を保持する第１の鍵保持部（１４０２）と、

前記第１の公開暗号鍵によって暗号化された第１の共通鍵（Ks1）を前記インタフェース部を介して外部から受けて、復号処理するための第１の復号処理部（１４０４）と、

前記記録装置ごとに異なる第２の公開暗号鍵（KPm(i)）を保持する第２の鍵保持部（１４１６）と、

前記コンテンツデータの通信ごとに更新される第２の共通鍵（Ks2）を生成するセッションキー発生部（１４１８）と、

前記第２の共通鍵および前記第２の公開暗号鍵を前記第１の共通鍵によって暗号化し、前記インタフェース部を介して外部に出力するための第１の暗号化処理部（１４０６）と、

前記インタフェース部を介して、前記第２の共通鍵および前記第２の公開暗号鍵によって暗号化された、少なくとも前記ライセンスキーを含む第１の再生情報

を受けて、前記第２の共通鍵によって復号するための第２の復号処理部（１４１２）と、

前記第２の公開暗号鍵によって暗号化されたデータを復号するための第２の秘密復号鍵（Km(i)）を保持する第３の鍵保持部（１４２１）と、

前記前記第２の秘密復号鍵による復号処理を実行するための第３の復号処理部（１４２２）と、

前記第１の再生情報および前記暗号化コンテンツデータを記録するための第１の記憶部（１４１５，１４４０）とを備える、記録装置。

３３．　前記コンテンツデータの通信の禁止対象とされる前記第１のクラス証明データ（Cmc(m)）をリストアップした禁止クラスリストを保持するための第２の記憶部（１４３０，２４１５）と、

前記コンテンツデータの配信動作が指示されるのに応じて、前記インタフェース部（１２０２）を介して外部から受けた情報に基づいて、前記第２の記憶部に保持される前記リストの内容を更新することが可能な制御部（１４２０）と、

外部から指示される、他の記録装置（１１２，１１６）に対して、少なくとも前記第１の再生情報を含むデータを移転するための移動動作に応じて、前記他の記録装置から暗号化された前記第１のクラス証明データ（Cmc(m)）を受けて、前記認証鍵（KPma）による復号を行なって前記正当性を確認するための認証処理部（１４０８）とをさらに備え、

前記制御部は、前記移動動作時において、前記認証処理部において得られた前記他の記録装置に対応する前記第１のクラス証明データが前記第２の記憶部に保持される前記禁止クラスリストに含まれている場合には、前記移動動作を中止する、請求の範囲第３２項に記載の記録装置。

３４．　認証処理部（１４０８）は、外部から指示される前記コンテンツデータの再生動作に応じて、前記認証鍵（KPma）によって暗号化された、前記コンテンツデータの再生回路（１５５０）に対応する第２のクラス証明データ（Cp(n)）を前記インタフェース部（１２０２）を介して受けて復号し、

前記禁止クラスリスト（CRL）は、禁止対象とされる前記第２のクラス証明データをさらにリストアップし、

前記制御部（１４２０）は、前記再生動作に応じて、前記認証処理部において得られた前記再生回路に対応する前記第２のクラス証明データが前記第２の記憶部に保持される前記禁止クラスリストに含まれている場合には、前記再生動作を中止する、請求の範囲第３３項に記載の記録装置。

３５．　前記第２の記憶部（１４３０，２１４５）は、第三者に読出不可能なセキュリティー領域（TRM）内に配置される、請求の範囲第３３項に記載の記録装置。

３６．　前記禁止クラスリスト（CRL）のデータを前記第２の公開暗号鍵（KPm(i)）で暗号化するための第２の暗号化処理部（１４２４）をさらに備え、

前記第２の記憶部（２４１５）は、第三者に読出不可能なセキュリティー領域（TRM）外に設けられて、前記第２の暗号化処理部によって暗号化された前記禁止クラスリストを保持する、請求の範囲第３３項に記載の記録装置。

３７．　前記記録装置ごとに異なる秘密鍵（K(i)）を保持する秘密鍵保持部（１４５０）と、

前記秘密鍵による暗号化を実行するための、秘密鍵暗号化処理部（１４５２）と、

前記秘密鍵で暗号化されたデータを復号するための秘密鍵復号処理部（１４５４）とをさらに備え、

前記第１の記憶部（１４１５）および前記第２の記憶部（２４１５）は、第三者に読出不可能なセキュリティー領域（TRM）外に設けられ、

前記第１の記憶部（１４１５）は、前記第２の暗号化処理部によって暗号化されたデータを保持し、

前記第２の記憶部（２４１５）は、前記第２の暗号化処理部によって暗号化された前記禁止クラスリストを保持する、請求の範囲第３３項に記載の記録装置。

３８．前記第１の記憶部（１４１５，１４４０）は、半導体メモリであり、

前記記録装置は、メモリカードである、請求の範囲第３２項に記載の記録装置。

３９．　記録装置であって、

データ（Kc）を記録するための第１の記憶部（１４１５，１４４０）と、

インタフェース部（１２０２）を介して入力される、認証鍵(KPma)によって

復号することで認証可能な状態に暗号化されたクラス証明データ（Cmc(m), Cp(n)）を受けて、前記認証鍵による復号を行なって正当性を確認するための認証処理部（１４０８）と、

前記データの出力を許可する対象となされるクラス証明データをリストアップした許可クラスリストを保持するための第２の記憶部と、

外部からの前記データの出力指示に応じて、前記インタフェース部を介した前記データの出力を制御する制御部（１４２０）とを備え、

前記制御部は、前記出力指示とともに外部から前記インタフェース部を介して入力される、前記暗号化がなされた前記クラス証明データを前記認証処理部で復号して得られる前記クラス証明データが前記許可クラスリストに含まれる場合において、前記データの出力を実行する、記録装置。

FIG.1

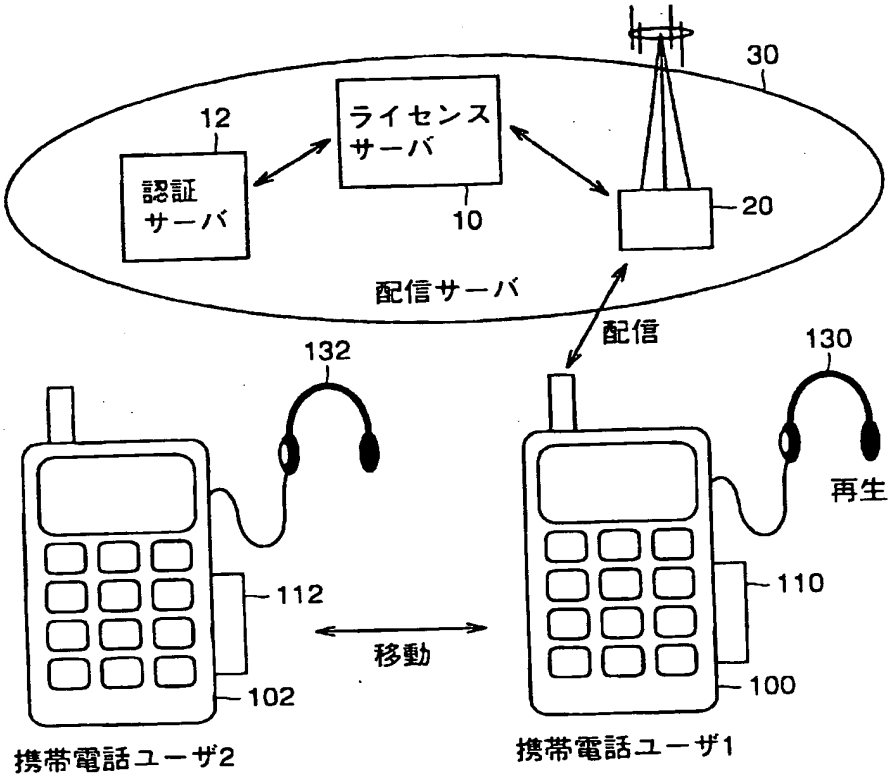

30
12
ライセンス
サーバ
認証
サーバ
10
20
配信サーバ
配信
132
130
再生
112
110
移動
102
100
携帯電話ユーザ2
携帯電話ユーザ1

FIG.2

名称	属性	保持／発生箇所	機能・特徴
Data	コンテンツデータ	配信サーバ	例：音楽データ
Kc	ライセンスキー		暗号化コンテンツデータの復号鍵
{Data}Kc	暗号化コンテンツデータ		共通鍵Kcで復号可能な暗号化が施されたコンテンツデータこの形式で配信サーバより配布。
Data-inf	付加情報		例：コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報
コンテンツID	コンテンツに関する情報		コンテンツデータDataを識別するコード
ライセンスID	ライセンスに関する情報		ライセンスの発行を特定できる管理コード（コンテンツIDを含めて識別することも可）
AC	ライセンス購入条件		利用者側から指定(例：ライセンス数,機能限定等)
AC1	アクセス制限情報		メモリのアクセスに対する制限(例：再生可能回数)
AC2	再生回路制御情報		コンテンツ再生回路(携帯電話機)における制御情報（例：再生可否）

FIG.3

名称	属性	保持／発生箇所	機能・特徴
CRL	禁止クラスリスト関連情報	配信サーバ メモリカード	禁止クラスリストの対象クラスデータ
CRL_dat		配信サーバ	禁止クラスリストのバージョン更新のための情報 （差分データ形式）
CRL_ver		メモリカード	禁止クラスリストのバージョン情報
KPp(n)	公開暗号化鍵 （非対称鍵）	携帯電話機	Kp(n)にて復号可能。 {KPp(n)//Cp(n)}KPmaの形式で出荷時に記録 ＊携帯電話機の種類ごと(n)に異なる情報を有する。
KPmc(m)	公開暗号化鍵 （非対称鍵）	メモリカード	Kmcにて復号可能。 {KPmc(m)//Cmc(m)}KPmaの形式で出荷時に記録 ＊メモリカードの種類ごと(m)に異なる情報を有する。
Kp(n)	秘密復号鍵	携帯電話機	コンテンツ再生回路（携帯電話機）固有の復号鍵 ＊携帯電話機の種類ごと(n)に異なる情報を有する。
Kmc(m)	秘密復号鍵	メモリカード	メモリカード固有の復号鍵 ＊メモリカードの種類ごと(m)に異なる情報を有する。
Cp(n)	クラス証明書	携帯電話機	コンテンツ再生回路のクラス証明書。認証機能を有する。 {KPp(n)//Cp(n)}KPmaの形式で出荷時に記録 ＊携帯電話機のクラスごと(n)に異なる情報を有する。
Cmc(m)		メモリカード	メモリカードのクラス証明書。認証機能を有する。 {KPmc(m)//Cmc(m)}KPmaの形式で出荷時に記録 ＊メモリカードのクラスごと(m)に異なる情報を有する。

FIG.4

名称	属性	保持／発生箇所	機能・特徴
Ks1	共通鍵（セッション固有）	配信サーバ	配信セッション毎に発生
Ks2		メモリカード	配信／移動(受)セッション毎に発生
Ks3		メモリカード	再生／移動(送)セッション毎に発生
Ks4		携帯電話機	再生セッション毎に発生
Km(i)	秘密復号鍵	メモリカード	メモリカードごと(i)に固有の復号鍵 KPm(i)で暗号化されたデータはKm(i)で復号可能
KPm(i)	公開暗号化鍵（非対称鍵）	メモリカード	メモリカードごと(i)に固有の暗号化鍵
KPma	復号鍵	配信サーバ	配信システム全体で共通。
Kcom	秘密復号鍵	携帯電話機 配信サーバ	再生回路共通の秘密鍵。Kc,AC2の暗号化および復号に利用。

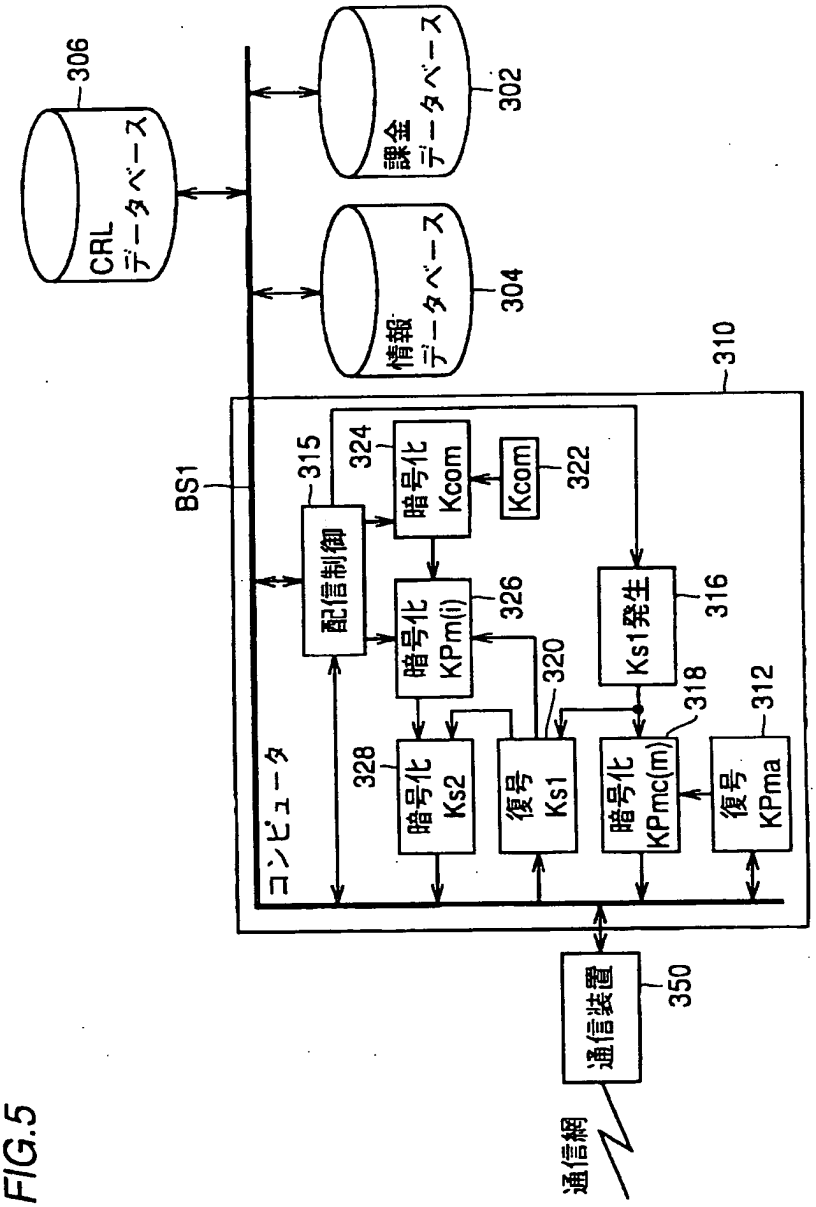

10
306
CRL
データベース
課金
データベース
302
情報
データベース
304
310
BS1
315
配信制御
324
暗号化
Kcom
Kcom
322
暗号化
KPm(i)
326
Ks1発生
316
320
318
328
暗号化
Ks2
復号
Ks1
暗号化
KPmc(m)
復号
KPma
312
コンピュータ
通信装置
350
通信網

FIG.5

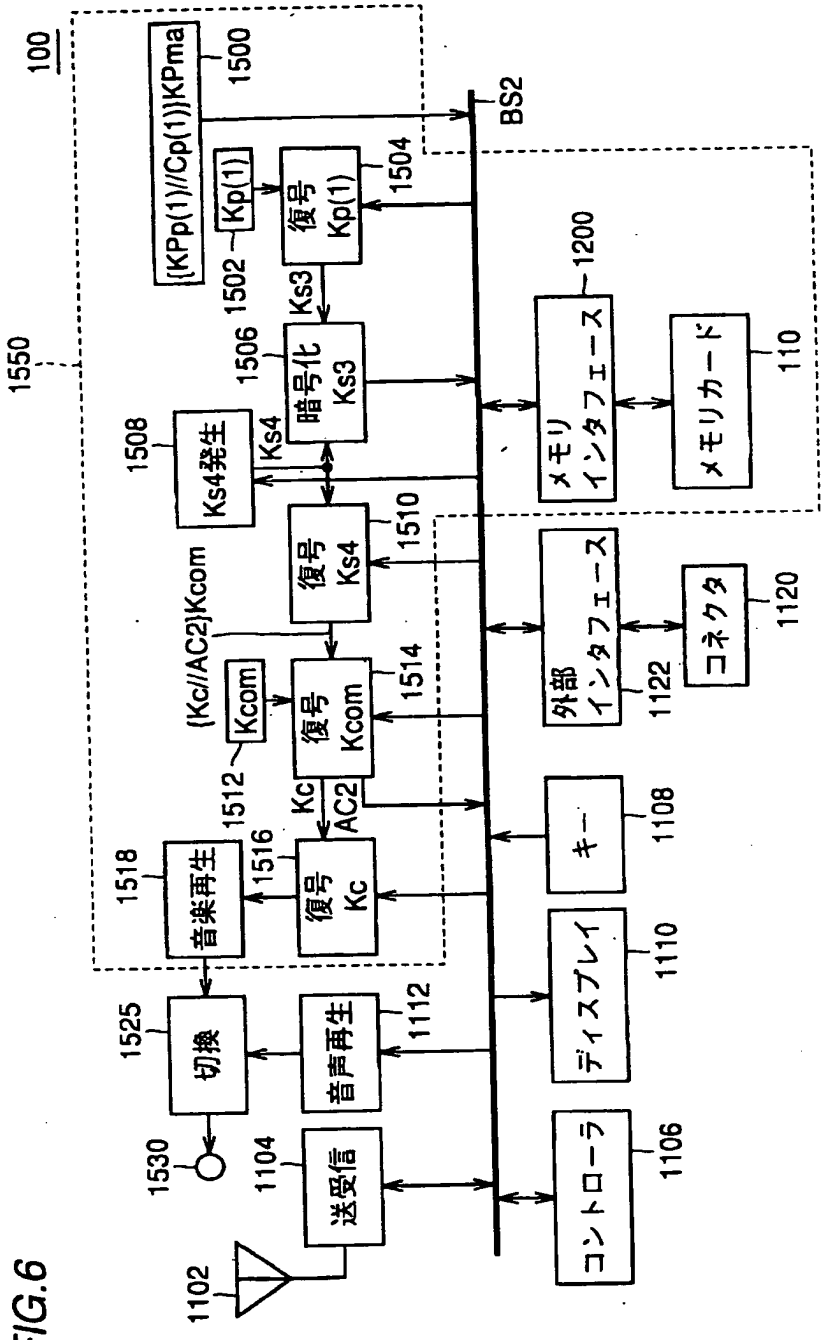

100
1550
[KPp(1)//Cp(1)]KPma
1500
BS2
Kp(1)
復号 Kp(1)
1504
1502
Ks3
暗号化 Ks3
1506
Ks4
Ks4発生
1508
復号 Ks4
1510
[Kc//AC2]Kcom
Kcom
復号 Kcom
1514
1512
Kc
AC2
復号 Kc
1516
音楽再生
1518
切換
1525
音声再生
1112
1530
送受信
1104
1102
メモリインタフェース
1200
メモリカード
110
外部インタフェース
1122
コネクタ
1120
キー
1108
ディスプレイ
1110
コントローラ
1106

FIG.6

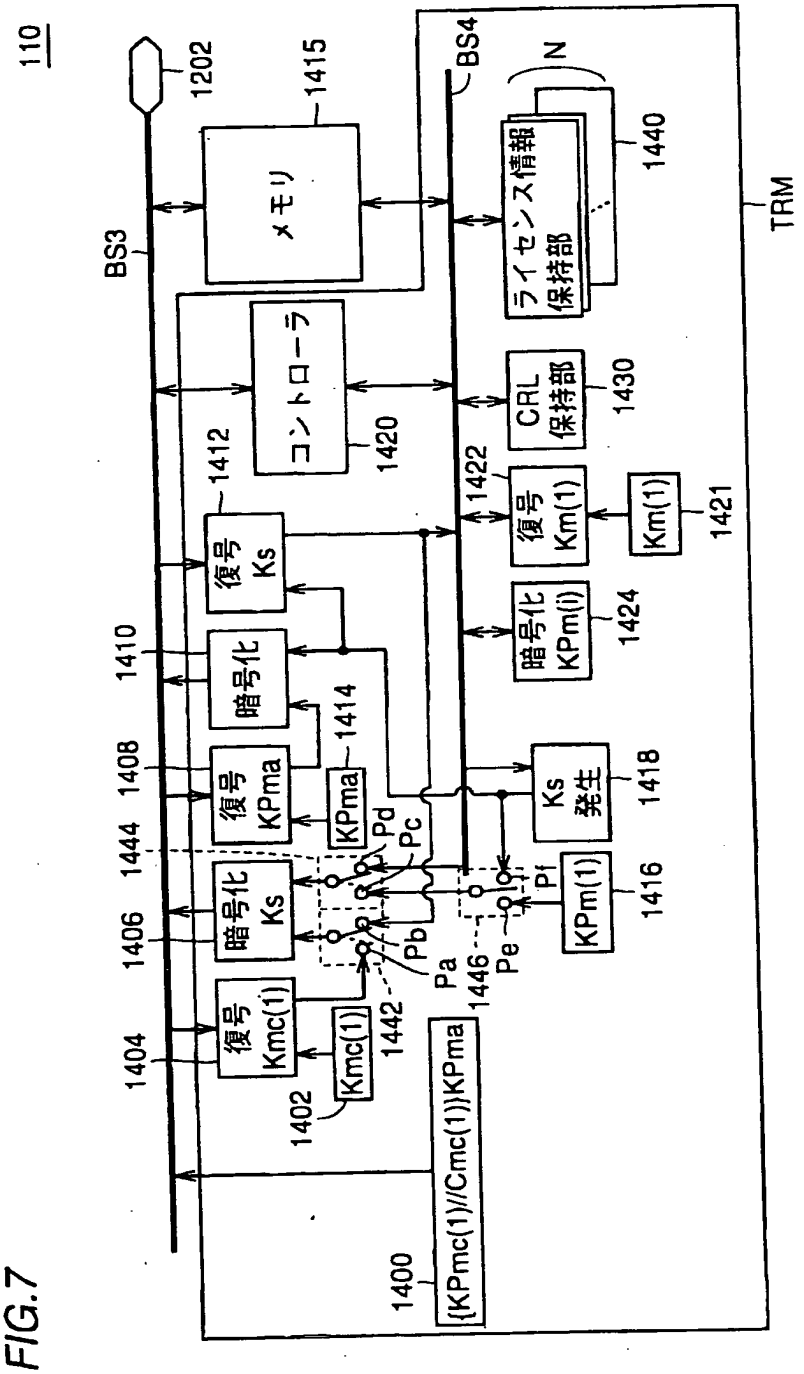

110
1202
1415
BS4
N
BS3
メモリ
ライセンス情報
保持部
1440
TRM
コントローラ
1420
CRL
保持部
1430
1412
1422
復号
Ks
復号
Km(1)
Km(1)
1421
1410
暗号化
KPm(i)
1424
暗号化
Ks
1408
復号
KPma
1414
KPma
Pd
Pc
Ks
発生
1418
1444
1406
Pb
Pf
KPm(1)
1416
Pa
Pe
1446
1404
復号
Kmc(1)
Kmc(1)
1442
1402
{KPmc(1)//Cmc(1)}KPma
1400

FIG.7

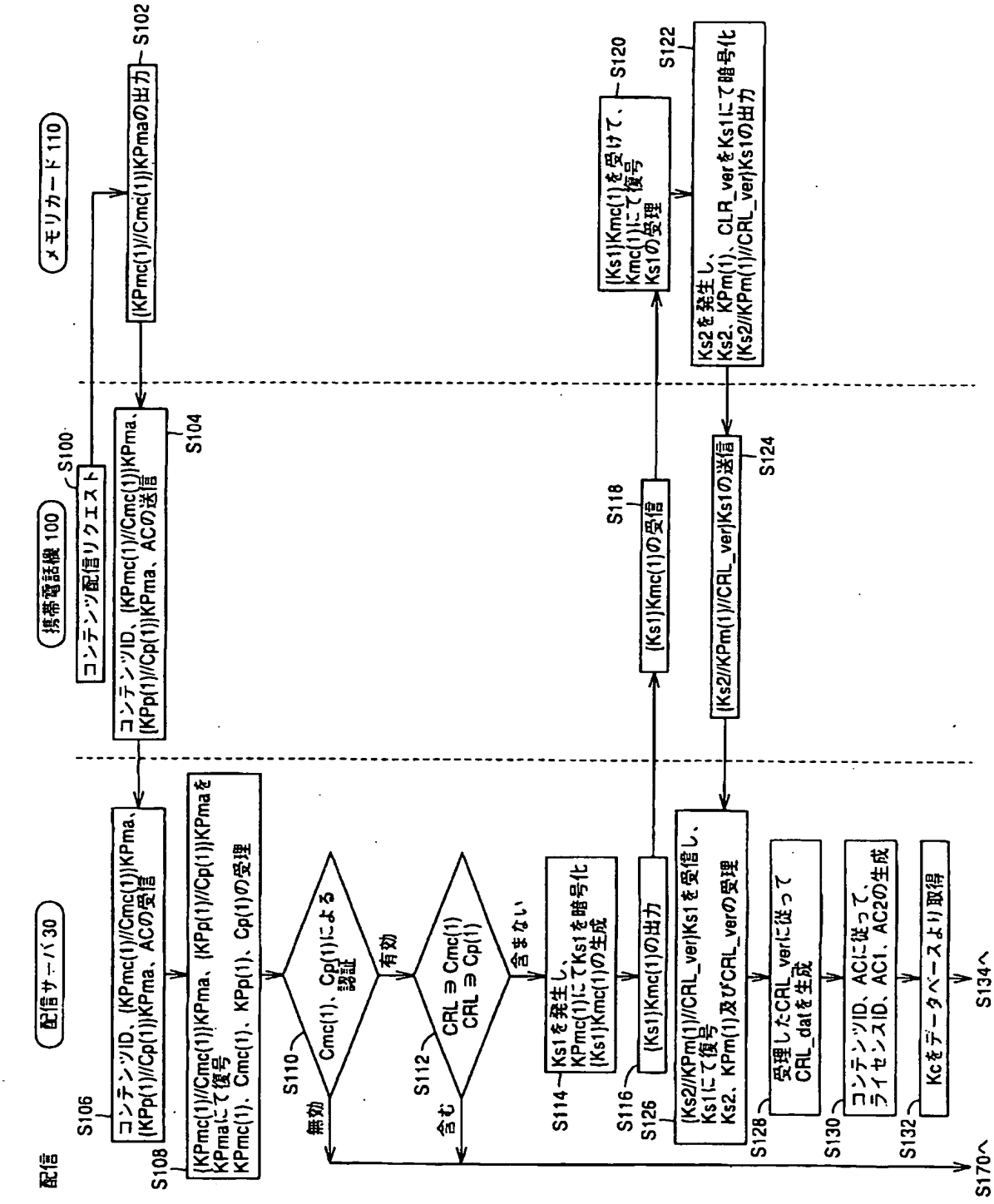

メモリカード110
携帯電話機100
配信サーバ30
配信
コンテンツ配信リクエスト
S100
{KPmc(1)//Cmc(1)}KPmaの出力
S102
コンテンツID、{KPmc(1)//Cmc(1)}KPma、{KPp(1)//Cp(1)}KPma、ACの送信
S104
コンテンツID、{KPmc(1)//Cmc(1)}KPma、ACの受信
S106
{KPmc(1)//Cmc(1)}KPma、{KPp(1)//Cp(1)}KPmaを{KPmc(1)//Cmc(1)}KPmaにて復号
S108
KPmc(1)、Cmc(1)、KPp(1)、Cp(1)の受理
Cmc(1)、Cp(1)による認証
S110
有効
無効
CRL ∋ Cmc(1)
CRL ∋ Cp(1)
S112
含む
含まない
Ks1を発生し、KPmc(1)にてKs1を暗号化{Ks1}Kmc(1)の生成
S114
{Ks1}Kmc(1)の出力
S116
{Ks1}Kmc(1)の受信
S118
{Ks1}Kmc(1)を受けて、Kmc(1)にて復号
Ks1の受理
S120
Ks2を発生し、Ks2、KPm(1)、CLR_verをKs1にて暗号化{Ks2//KPm(1)//CRL_ver}Ks1の出力
S122
{Ks2//KPm(1)//CRL_ver}Ks1の送信
S124
{Ks2//KPm(1)//CRL_ver}Ks1を受信し、Ks1にて復号
Ks2、KPm(1)及びCRL_verの受理
S126
受理したCRL_verに従ってCRL_datを生成
S128
コンテンツID、ACに従って、ライセンスID、AC1、AC2の生成
S130
Kcをデータベースより取得
S132
S134へ
S170へ

FIG.8

FIG.9

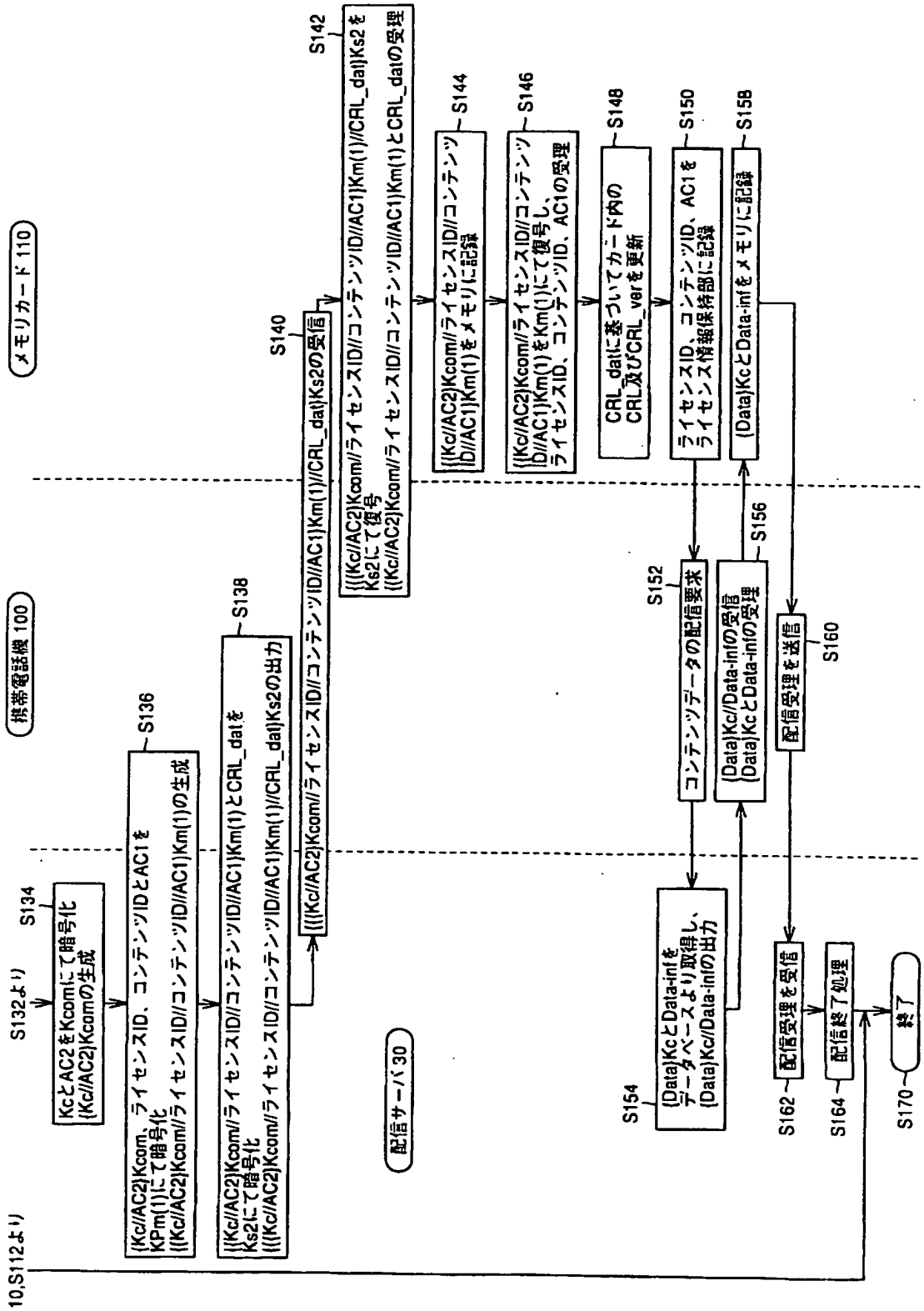

メモリカード 110
携帯電話機 100
配信サーバ 30
S110,S112より
S132より
S134
KcとAC2をKcomにて暗号化
{Kc//AC2}Kcom
S136
{Kc//AC2}Kcom、ライセンスIDとAC1を
KPm(1)にて暗号化
{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(1)の生成
S138
{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(1)とCRL_dat1を
Ks2にて暗号化
{{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(1)//CRL_dat1}Ks2の出力
S140
{{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(1)//CRL_dat1}Ks2の受信
S142
{{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(1)//CRL_dat1}Ks2を
Ks2にて復号
{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(1)とCRL_datの受理
S144
{{Kc//AC2}Kcom//ライセンスID//コンテンツ
ID//AC1}Km(1)をメモリに記録
S146
{{Kc//AC2}Kcom//ライセンスID//コンテンツ
ID//AC1}Km(1)をKm(1)にて復号し、
ライセンスID、コンテンツID、AC1の受理
S148
CRL_datに基づいてカード内の
CRL及びCRL_verを更新
S150
ライセンスID、コンテンツID、AC1を
ライセンス情報保持部に記録
S158
{Data}KcとData-infをメモリに記録
S152
コンテンツデータの配信要求
S154
{Data}KcとData-infを
データベースより取得し、
{Data}Kc//Data-infの出力
S156
{Data}Kc//Data-infの受信
{Data}KcとData-infの受理
S160
配信受理を送信
S162
配信受理を受信
S164
配信終了処理
S170
終了

FIG.10

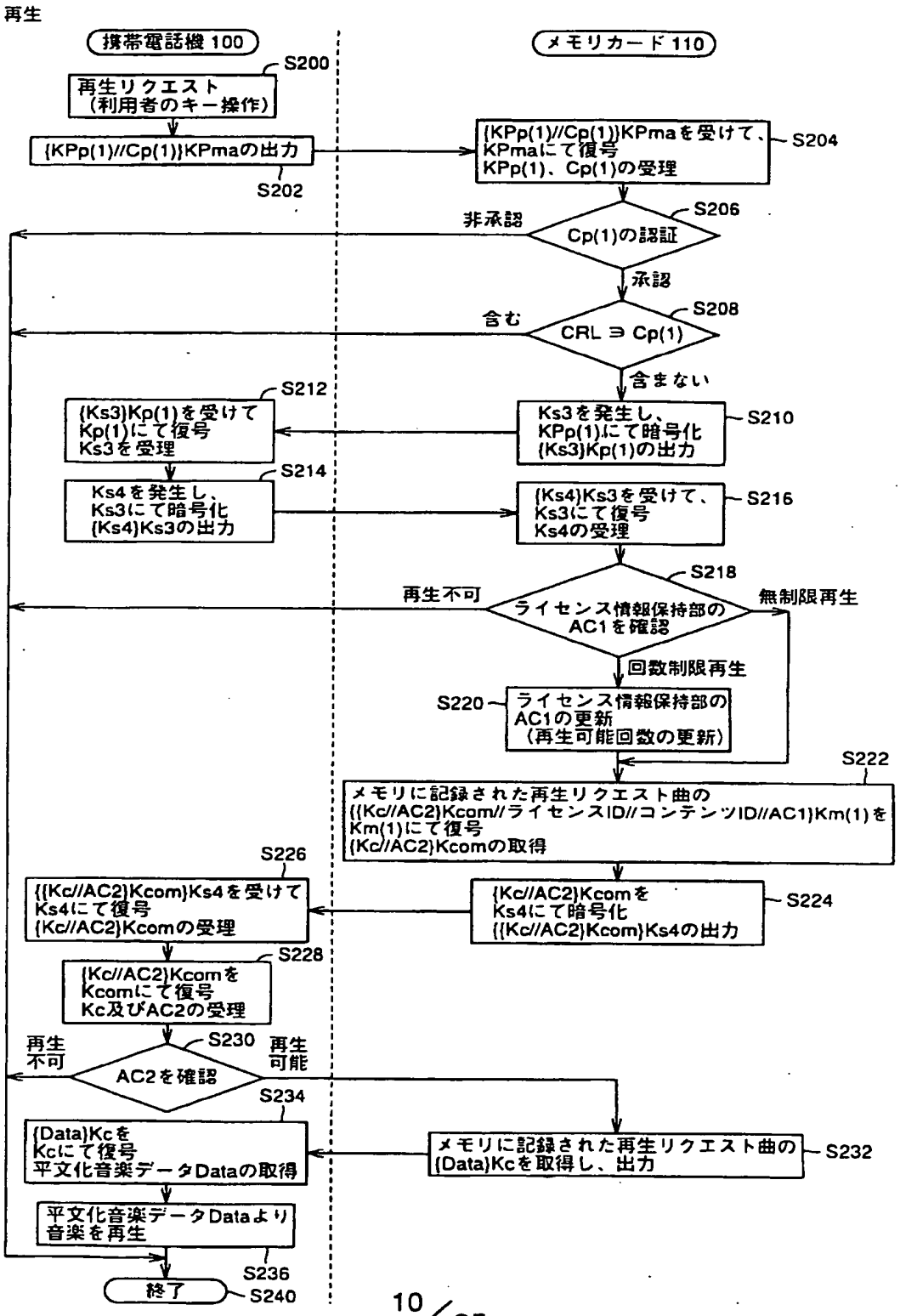

再生
携帯電話機 100
メモリカード 110
S200
再生リクエスト
(利用者のキー操作)
{KPp(1)//Cp(1)}KPmaの出力
S202
{KPp(1)//Cp(1)}KPmaを受けて、
KPmaにて復号
KPp(1)、Cp(1)の受理
S204
S206
非承認
Cp(1)の認証
承認
S208
含む
CRL ∋ Cp(1)
含まない
S212
{Ks3}Kp(1)を受けて
Kp(1)にて復号
Ks3を受理
Ks3を発生し、
KPp(1)にて暗号化
{Ks3}Kp(1)の出力
S210
S214
Ks4を発生し、
Ks3にて暗号化
{Ks4}Ks3の出力
{Ks4}Ks3を受けて、
Ks3にて復号
Ks4の受理
S216
S218
再生不可
ライセンス情報保持部の
AC1を確認
無制限再生
回数制限再生
S220
ライセンス情報保持部の
AC1の更新
(再生可能回数の更新)
S222
メモリに記録された再生リクエスト曲の
{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(1)を
Km(1)にて復号
{Kc//AC2}Kcomの取得
S226
{{Kc//AC2}Kcom}Ks4を受けて
Ks4にて復号
{Kc//AC2}Kcomの受理
{Kc//AC2}Kcomを
Ks4にて暗号化
{{Kc//AC2}Kcom}Ks4の出力
S224
S228
{Kc//AC2}Kcomを
Kcomにて復号
Kc及びAC2の受理
再生
不可
S230
AC2を確認
再生
可能
S234
{Data}Kcを
Kcにて復号
平文化音楽データDataの取得
メモリに記録された再生リクエスト曲の
{Data}Kcを取得し、出力
S232
平文化音楽データDataより
音楽を再生
S236
終了
S240

FIG.11

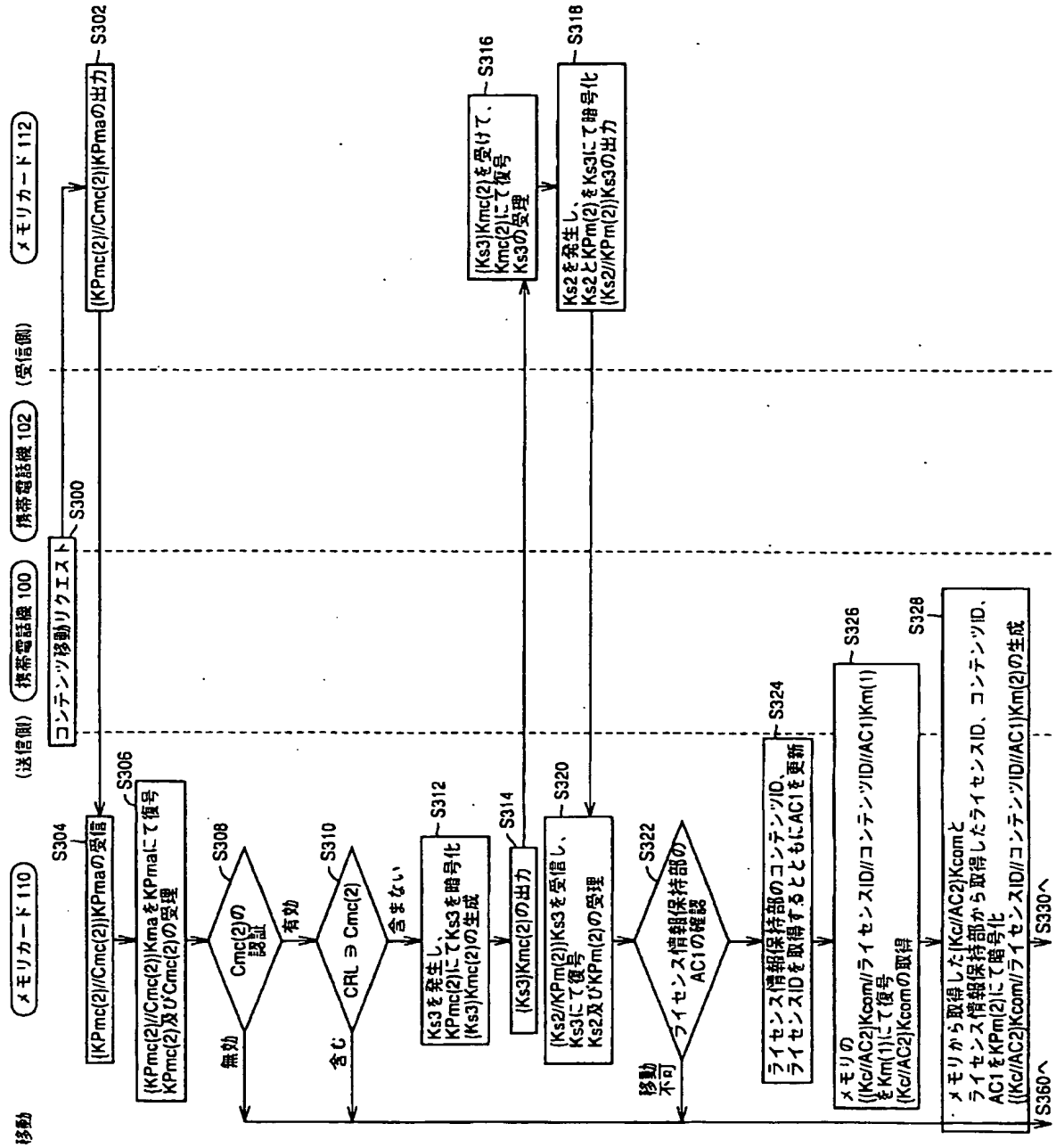
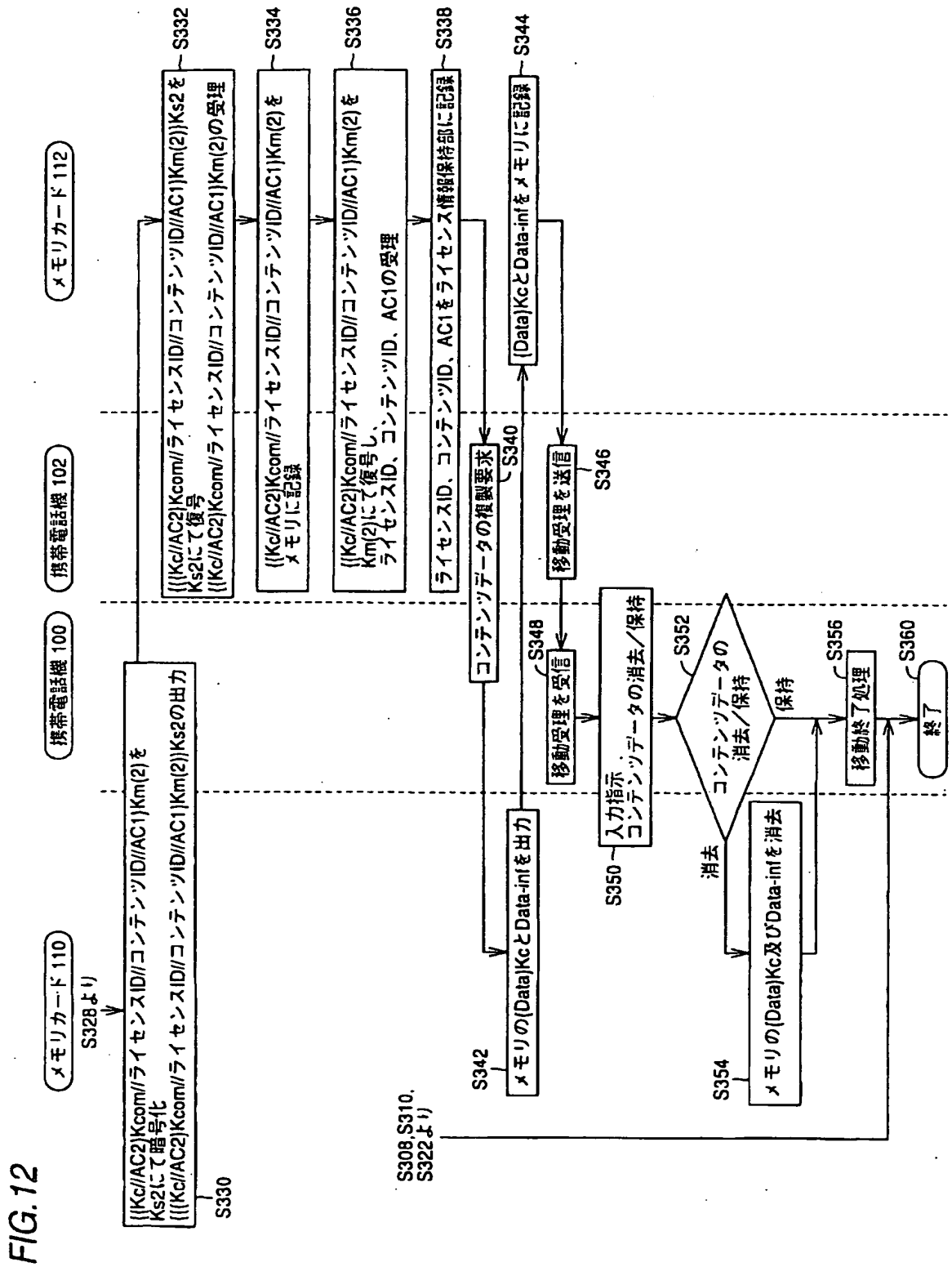

移動
メモリカード110
(送信側)
携帯電話機100
携帯電話機102
(受信側)
メモリカード112
コンテンツ移動リクエスト
S300
{KPmc(2)//Cmc(2)}KPmaの出力
S302
{KPmc(2)//Cmc(2)}KPmaの受信
S304
{KPmc(2)//Cmc(2)}KmaをKPmaにて復号
KPmc(2)及びCmc(2)の受理
S306
Cmc(2)の認証
S308
無効
有効
CRL ∋ Cmc(2)
S310
含む
含まない
Ks3を発生し、
KPmc(2)にてKs3を暗号化
{Ks3}Kmc(2)の生成
S312
{Ks3}Kmc(2)の出力
S314
{Ks3}Kmc(2)を受けて、
Kmc(2)にて復号
Ks3の受理
S316
{Ks2/KPm(2)}Ks3を受信し、
Ks3にて復号
Ks2及びKPm(2)の受理
S320
Ks2を発生し、
Ks2とKPm(2)をKs3にて暗号化
{Ks2//KPm(2)}Ks3の出力
S318
ライセンス情報保持部のAC1の確認
S322
移動不可
ライセンス情報保持部のコンテンツID、
ライセンスIDを取得するとともにAC1を更新
S324
メモリの
{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(1)
をKm(1)にて復号
{Kc//AC2}Kcomの取得
S326
S328
・メモリから取得した{Kc//AC2}Kcomと
ライセンス情報保持部から取得したライセンスID、コンテンツID、
AC1をKPm(2)にて暗号化
{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(2)の生成
S360へ
S330へ

FIG.12


メモリカード 110
携帯電話機 100
携帯電話機 102
メモリカード 112
S328より
{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(2)を
Ks2にて暗号化
{{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(2)}Ks2の出力
S330
{{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(2)}Ks2を
Ks2にて復号
{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(2)の受理
S332
{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(2)を
メモリに記録
S334
{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(2)を
Km(2)にて復号し、
ライセンスID、コンテンツID、AC1の受理
S336
ライセンスID、コンテンツID、AC1をライセンス情報保持部に記録
S338
{Data}KcとData-infをメモリに記録
S344
コンテンツデータの複製要求
S340
移動受理を送信
S346
移動受理を受信
S348
入力指示
コンテンツデータの消去／保持
S350
S352
コンテンツデータの
消去／保持
消去
保持
S354
メモリの{Data}Kc及びData-infを消去
S356
移動終了処理
S360
終了
S308,S310,
S322より
S342
メモリの{Data}KcとData-infを出力

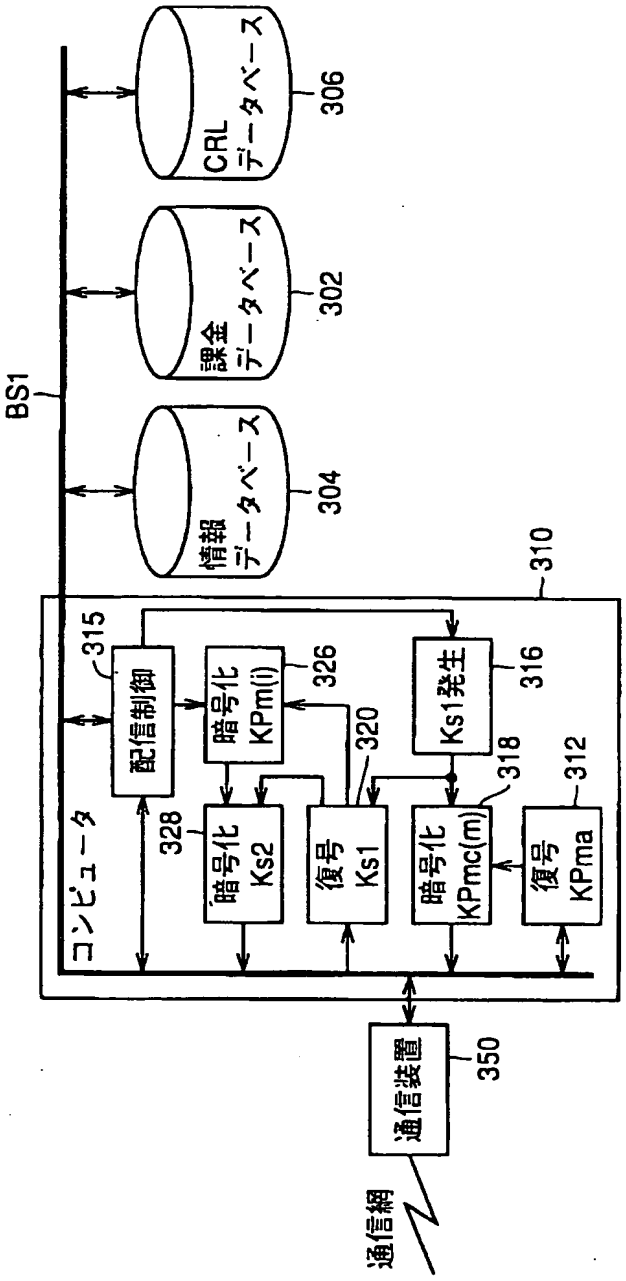

11
BS1
CRL データベース
306
課金 データベース
302
情報 データベース
304
310
コンピュータ
315
配信制御
暗号化 KPm(i)
326
320
Ks1発生
316
318
328
暗号化 Ks2
復号 Ks1
暗号化 KPmc(m)
復号 KPma
312
通信装置
350
通信網

FIG.13

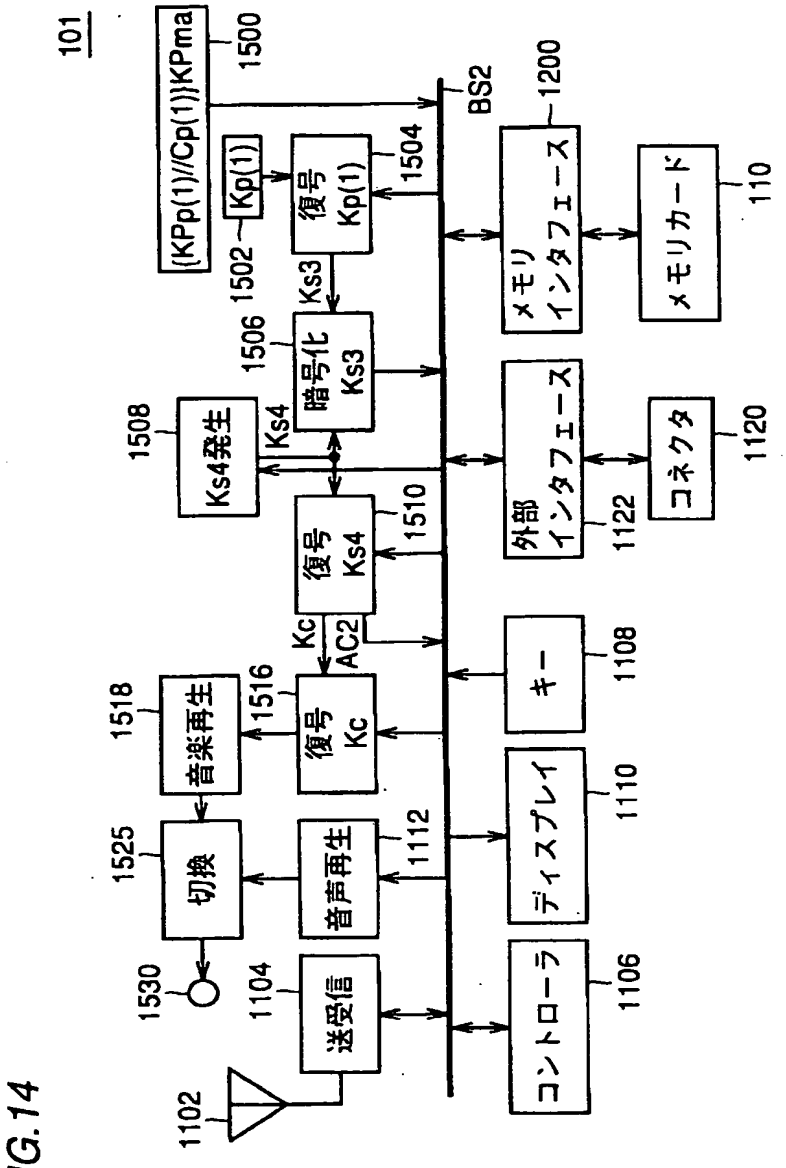

101
[(KPp(1)//Cp(1))]KPma
1500
BS2
1200
メモリ
インタフェース
メモリカード
110
Kp(1)
1502
復号
Kp(1)
1504
Ks3
1506
暗号化
Ks3
1508
Ks4発生
Ks4
復号
Ks4
1510
外部
インタフェース
1122
コネクタ
1120
Kc
AC2
1518
音楽再生
1516
復号
Kc
キー
1108
1525
切換
音声再生
1112
ディスプレイ
1110
1530
1104
送受信
コントローラ
1106
1102

FIG.14

FIG.15

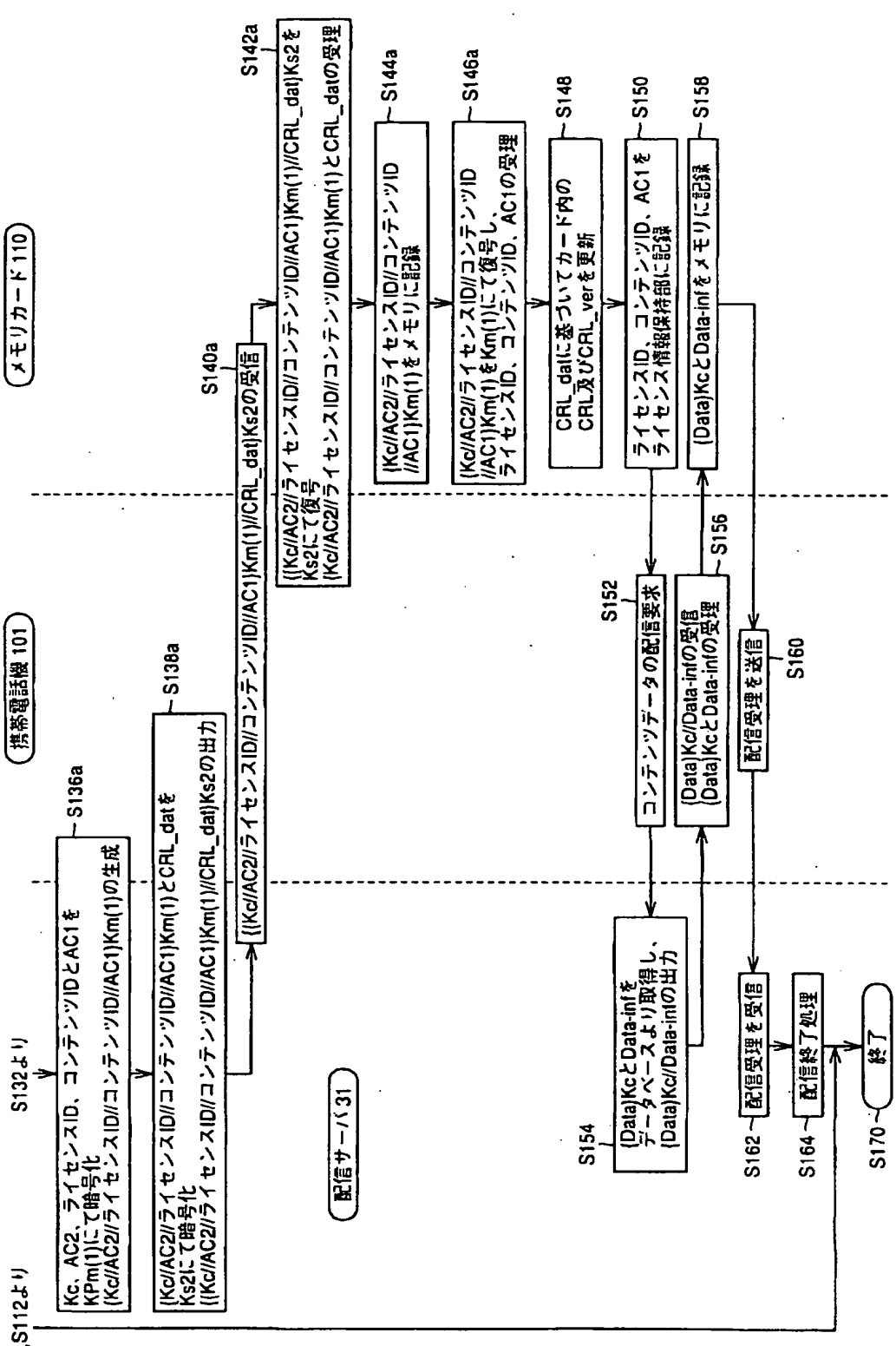
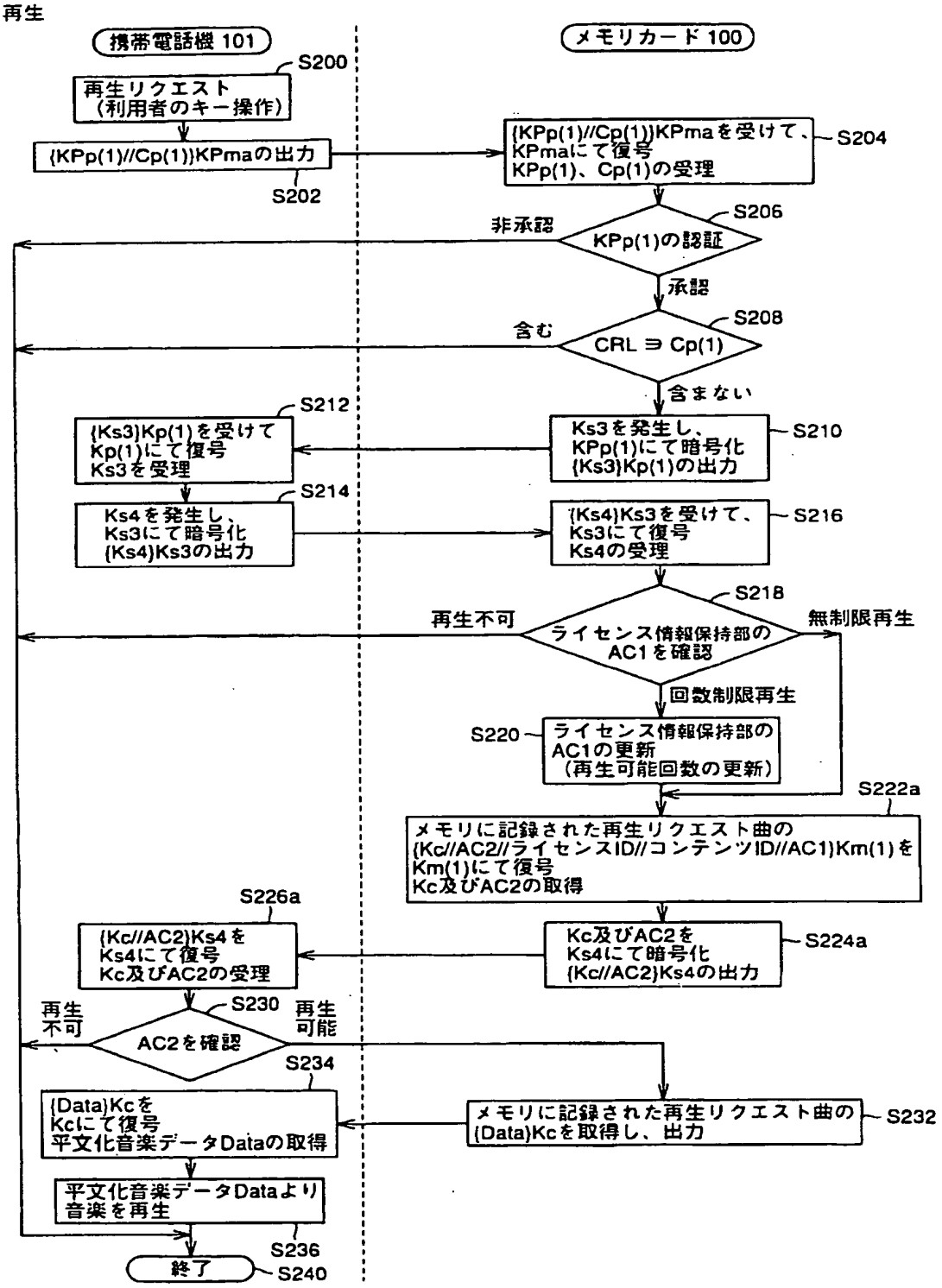

配信
(一部のみ)
S110,S112より
携帯電話機 101
メモリカード 110
配信サーバ 31
S132より
S136a
Kc、AC2、ライセンスID、コンテンツIDとAC1を
KPm(1)にて暗号化
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km(1)の生成
S138a
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km(1)とCRL_datを
Ks2にて暗号化
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km(1)//CRL_dat}Ks2の出力
S140a
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km(1)//CRL_dat}Ks2の受信
S142a
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km(1)//CRL_dat}Ks2を
Ks2にて復号
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km(1)とCRL_datの受理
S144a
{Kc//AC2//ライセンスID//コンテンツID
//AC1}Km(1)をメモリに記録
S146a
{Kc//AC2//ライセンスID//コンテンツID
//AC1}Km(1)をKm(1)にて復号し、
ライセンスID、コンテンツID、AC1の受理
S148
CRL_datに基づいてカード内の
CRL及びCRL_verを更新
S150
ライセンスID、コンテンツID、AC1を
ライセンス情報保持部に記録
S158
{Data}KcとData-infをメモリに記録
S152
コンテンツデータの配信要求
S154
{Data}KcとData-infを
データベースより取得し、
{Data}Kc//Data-infの出力
S156
{Data}Kc//Data-infの受信
{Data}KcとData-infの受理
S160
配信受理を送信
S162
配信受理を受信
S164
配信終了処理
S170
終了

FIG.16


再生
携帯電話機 101
メモリカード 100
S200
再生リクエスト
(利用者のキー操作)
{KPp(1)//Cp(1)}KPmaの出力
S202
{KPp(1)//Cp(1)}KPmaを受けて、
KPmaにて復号
KPp(1)、Cp(1)の受理
S204
S206
KPp(1)の認証
非承認
承認
S208
CRL ∋ Cp(1)
含む
含まない
S210
Ks3を発生し、
KPp(1)にて暗号化
{Ks3}Kp(1)の出力
S212
{Ks3}Kp(1)を受けて
Kp(1)にて復号
Ks3を受理
S214
Ks4を発生し、
Ks3にて暗号化
{Ks4}Ks3の出力
S216
{Ks4}Ks3を受けて、
Ks3にて復号
Ks4の受理
S218
ライセンス情報保持部の
AC1を確認
再生不可
無制限再生
回数制限再生
S220
ライセンス情報保持部の
AC1の更新
(再生可能回数の更新)
S222a
メモリに記録された再生リクエスト曲の
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km(1)を
Km(1)にて復号
Kc及びAC2の取得
S224a
Kc及びAC2を
Ks4にて暗号化
{Kc//AC2}Ks4の出力
S226a
{Kc//AC2}Ks4を
Ks4にて復号
Kc及びAC2の受理
S230
AC2を確認
再生不可
再生可能
S232
メモリに記録された再生リクエスト曲の
{Data}Kcを取得し、出力
S234
{Data}Kcを
Kcにて復号
平文化音楽データDataの取得
平文化音楽データDataより
音楽を再生
S236
終了
S240

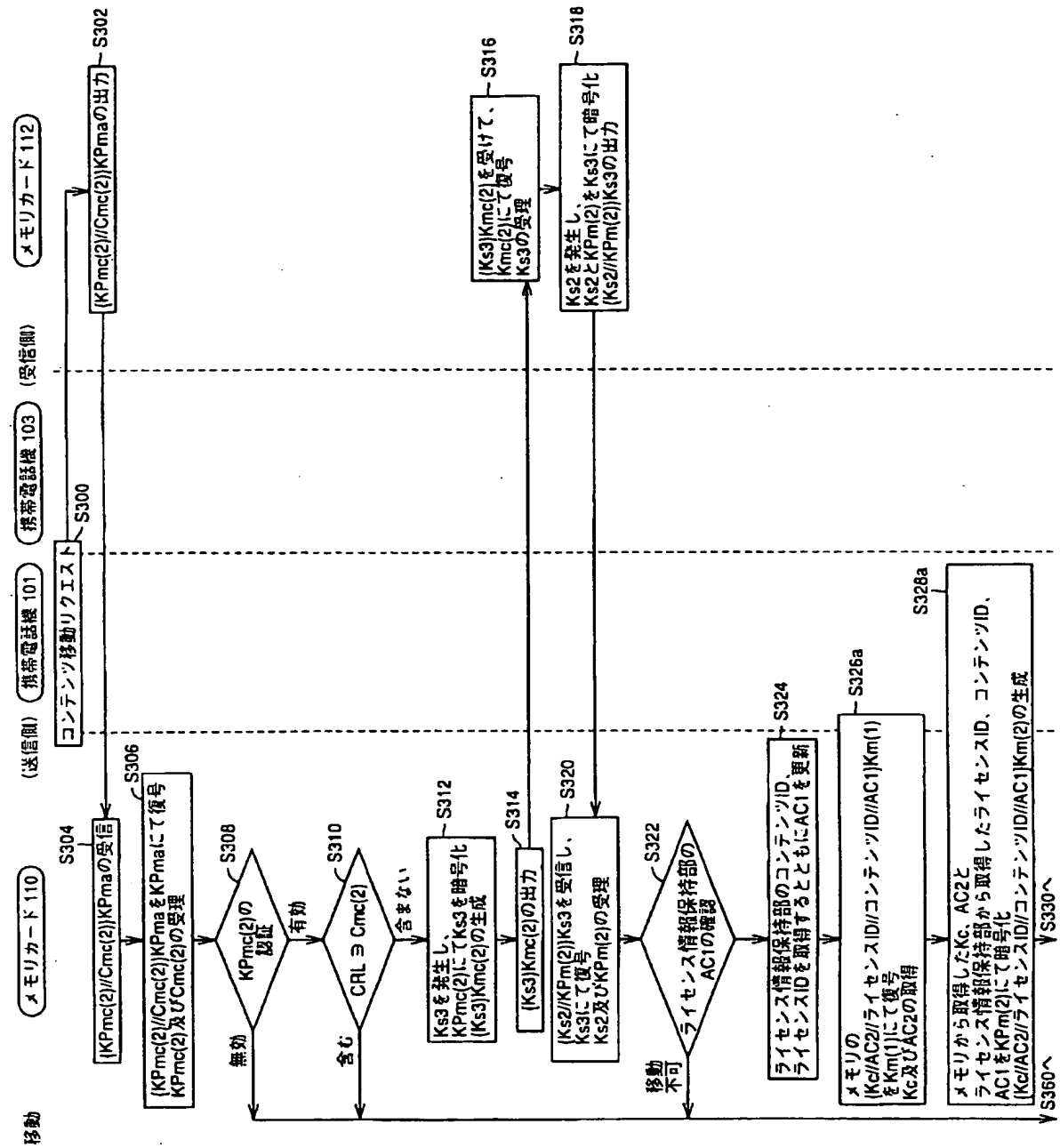
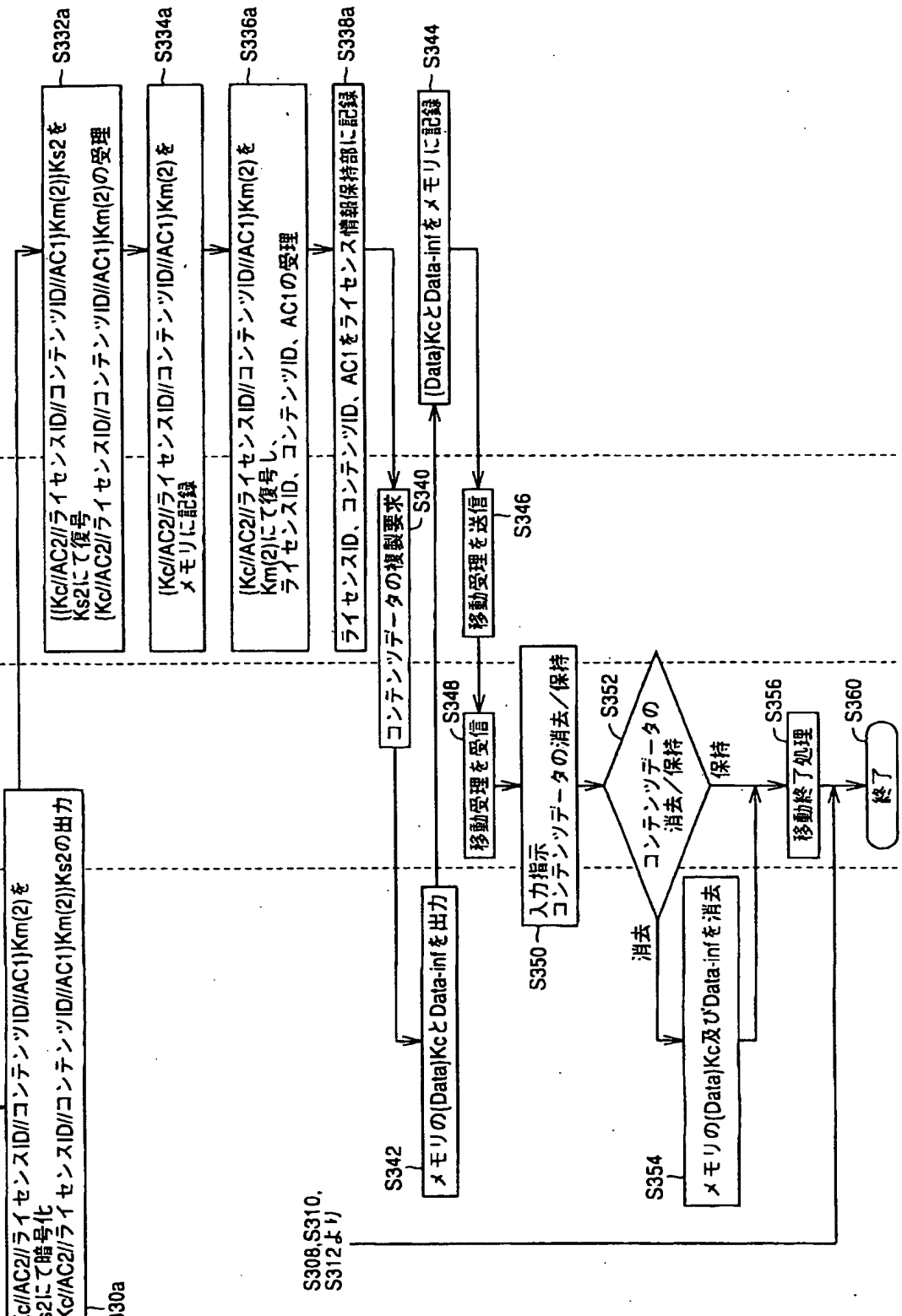

移動
メモリカード110
(送信側)
携帯電話機101
携帯電話機103
(受信側)
メモリカード112
コンテンツ移動リクエスト
S300
S302
S304
S306
S308
S310
S312
S314
S316
S318
S320
S322
S324
S326a
S328a
S330へ
S360へ
(KPmc(2)//Cmc(2))KPmaの出力
(KPmc(2)//Cmc(2))KPmaの受信
(KPmc(2)//Cmc(2))KPmaをKPmaにて復号
KPmc(2)及びCmc(2)の受理
KPmc(2)の認証
無効
有効
CRL ∋ Cmc(2)
含む
含まない
Ks3を発生し、
KPmc(2)にてKs3を暗号化
(Ks3)Kmc(2)の生成
(Ks3)Kmc(2)の出力
(Ks3)Kmc(2)を受けて、
Kmc(2)にて復号
Ks3の受理
Ks2を発生し、
Ks2とKPm(2)をKs3にて暗号化
(Ks2//KPm(2))Ks3の出力
(Ks2//KPm(2))Ks3を受信し、
Ks3にて復号
Ks2及びKPm(2)の受理
ライセンス情報保持部の
AC1の確認
移動不可
ライセンス情報保持部のコンテンツID、
ライセンスIDを取得するとともにAC1を更新
メモリの
(Kc//AC2//ライセンスID//コンテンツID//AC1)Km(1)
をKm(1)にて復号
Kc及びAC2の取得
メモリから取得したKc、AC2と
ライセンス情報保持部から取得したライセンスID、コンテンツID、
AC1をKPm(2)にて暗号化
(Kc//AC2//ライセンスID//コンテンツID//AC1)Km(2)の生成

FIG.17

FIG.18


メモリカード110
携帯電話機101
携帯電話機103
メモリカード112
S328aより
[Kc//AC2//ライセンスID//コンテンツID//AC1)Km(2)を
Ks2にて暗号化
((Kc//AC2//ライセンスID//コンテンツID//AC1)Km(2))Ks2の出力
S330a
((Kc//AC2//ライセンスID//コンテンツID//AC1)Km(2))Ks2を
Ks2にて復号
(Kc//AC2//ライセンスID//コンテンツID//AC1)Km(2)の受理
S332a
(Kc//AC2//ライセンスID//コンテンツID//AC1)Km(2)を
メモリに記録
S334a
(Kc//AC2//ライセンスID//コンテンツID//AC1)Km(2)を
Km(2)にて復号し、
ライセンスID、コンテンツID、AC1の受理
S336a
ライセンスID、コンテンツID、AC1をライセンス情報保持部に記録
S338a
コンテンツデータの複製要求
S340
(Data)KcとData-infをメモリに記録
S344
移動受理を送信
S346
移動受理を受信
S348
入力指示
コンテンツデータの消去／保持
S350
コンテンツデータの
消去／保持
S352
消去
保持
移動終了処理
S356
終了
S360
メモリの(Data)KcとData-infを出力
S342
メモリの(Data)Kc及びData-infを消去
S354
S308,S310,
S312より

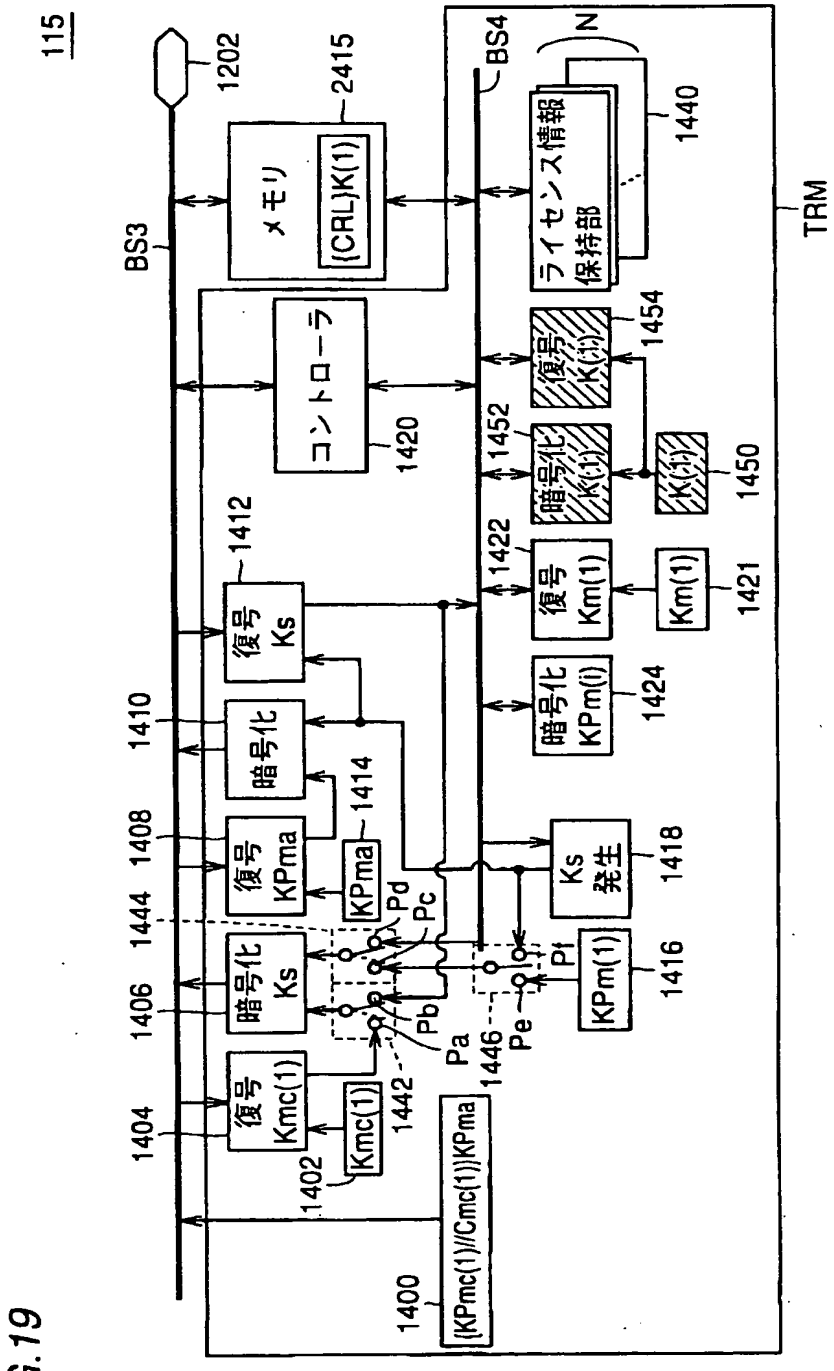

115
1202
2415
メモリ
(CRL)K(1)
BS3
BS4
N
ライセンス情報保持部
1440
TRM
コントローラ
1420
復号K(i)
1454
暗号化K(i)
1452
K(i)
1450
1422
復号Km(1)
Km(1)
1421
暗号化KPm(i)
1424
1412
復号Ks
1410
暗号化
1414
1408
復号KPma
KPma
Pd
Pc
1444
暗号化Ks
1406
Pb
Pa
1446
Pe
Pf
Ks発生
1418
KPm(1)
1416
復号Kmc(1)
1404
Kmc(1)
1442
1402
[KPmc(1)//Cmc(1)]KPma
1400

FIG.19

FIG.20

名称	属性	保持／発生箇所	機能・特徴
Ks1	共通鍵（セッション固有）	配信サーバ	配信セッション毎に発生
Ks2		メモリカード	配信／移動(受)セッション毎に発生
Ks3		メモリカード	再生／移動(送)セッション毎に発生
Ks4		携帯電話機	再生セッション毎に発生
Km(i)	秘密復号鍵	メモリカード	メモリカードごと(i)に固有の復号鍵 KPm(I)で暗号化されたデータはKm(i)で復号可能
KPm(i)	公開暗号化鍵（非対称鍵）	メモリカード	メモリカードごと(i)に固有の暗号化鍵
KPma	公開復号鍵	配信サーバ	配信システム全体で共通。
Kcom	秘密共通鍵	携帯電話機	再生回路共通の秘密鍵。Kc,AC2の暗号化および復号に利用。
K(i)	秘密鍵（対称鍵）	メモリカード	メモリカードごとに固有の秘密鍵 (i)はメモリカードを識別する引数 対称鍵なので高速に復号可能

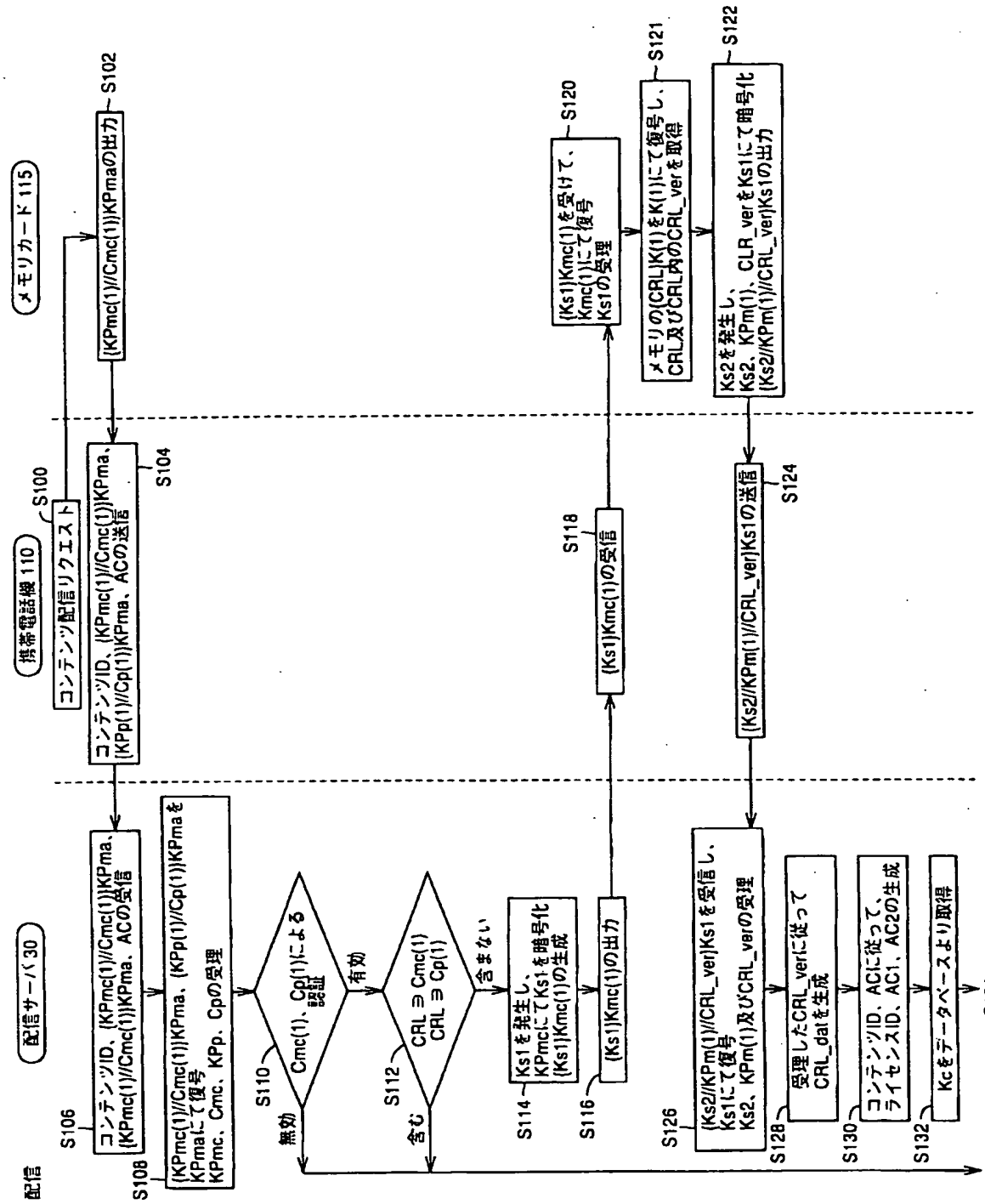

メモリカード115
携帯電話機110
配信サーバ30
配信
コンテンツ配信リクエスト
S100
{KPmc(1)//Cmc(1)}KPmaの出力
S102
コンテンツID、{KPmc(1)//Cmc(1)}KPma、{KPp(1)//Cp(1)}KPma、ACの送信
S104
コンテンツID、{KPmc(1)//Cmc(1)}KPma、ACの受信
S106
{KPmc(1)//Cmc(1)}KPmaを{KPmc(1)//Cmc(1)}KPmaにて復号
KPmc、Cmc、KPp、Cpの受理
S108
Cmc(1)、Cp(1)による認証
S110
無効
有効
CRL ∋ Cmc(1)
CRL ∋ Cp(1)
S112
含む
含まない
Ks1を発生し、KPmcにてKs1を暗号化{Ks1}Kmc(1)の生成
S114
{Ks1}Kmc(1)の出力
S116
{Ks1}Kmc(1)の受信
S118
{Ks1}Kmc(1)を受けて、Kmc(1)にて復号Ks1の受理
S120
メモリの{CRL}K(1)をK(1)にて復号し、CRL及びCRL内のCRL_verを取得
S121
Ks2を発生し、Ks2、KPm(1)、CLR_verをKs1にて暗号化{Ks2//KPm(1)//CRL_ver}Ks1の出力
S122
{Ks2//KPm(1)//CRL_ver}Ks1の送信
S124
{Ks2//KPm(1)//CRL_ver}Ks1を受信し、Ks1にて復号Ks2、KPm(1)及びCRL_verの受理
S126
受理したCRL_verに従ってCRL_datを生成
S128
コンテンツID、ACに従って、ライセンスID、AC1、AC2の生成
S130
Kcをデータベースより取得
S132
S134へ
S170へ

FIG.21

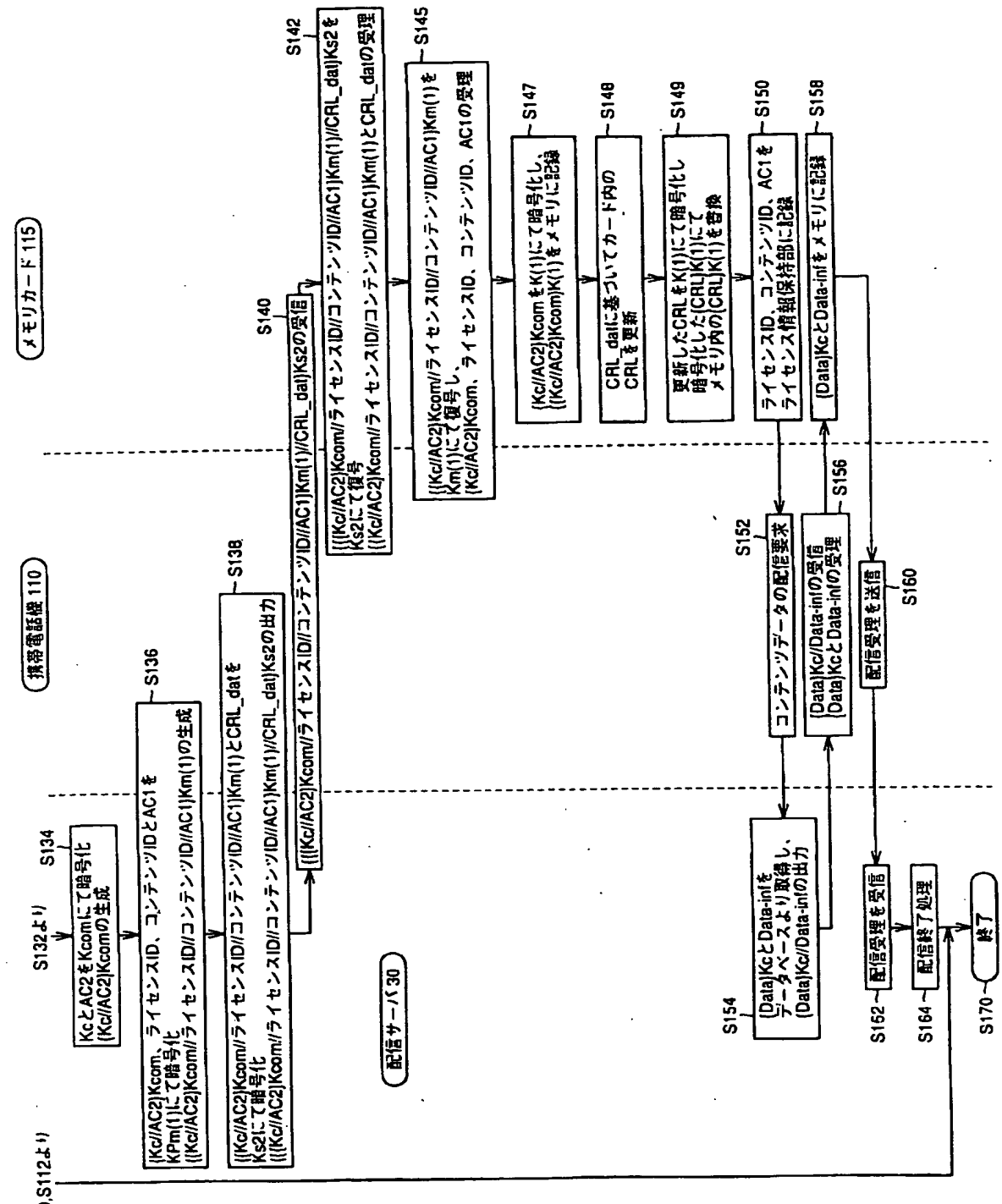

メモリカード115
携帯電話機110
配信サーバ30
S110,S112より
S132より
S134
KcとAC2をKcomにて暗号化
{Kc//AC2}Kcomの生成
S136
{Kc//AC2}Kcom、ライセンスIDとAC1を
KPm(1)にて暗号化
{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(1)の生成
S138
{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(1)とCRL_datを
Ks2にて暗号化
{{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(1)//CRL_dat}Ks2の出力
S140
{{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(1)//CRL_dat}Ks2の受信
S142
{{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(1)//CRL_dat}Ks2を
Ks2にて復号
{{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(1)とCRL_datの受理
S145
{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(1)を
Km(1)にて復号し、
{Kc//AC2}Kcom、ライセンスID、コンテンツID、AC1の受理
S147
{Kc//AC2}KcomをK(1)にて暗号化し、
{Kc//AC2}Kcom)K(1)をメモリに記録
S148
CRL_datに基づいてカード内の
CRLを更新
S149
更新したCRLをK(1)にて暗号化し
暗号化した{CRL}K(1)にて
メモリ内の{CRL}K(1)を置換
S150
ライセンスID、コンテンツID、AC1を
ライセンス情報保持部に記録
S158
{Data}KcとData-infをメモリに記録
S152
コンテンツデータの配信要求
S154
{Data}KcとData-infを
データベースより取得し、
{Data}Kc//Data-infの出力
S156
{Data}Kc//Data-infの受信
{Data}KcとData-infの受理
S160
配信受理を送信
S162
配信受理を受信
S164
配信終了処理
S170
終了

FIG.22

FIG.23

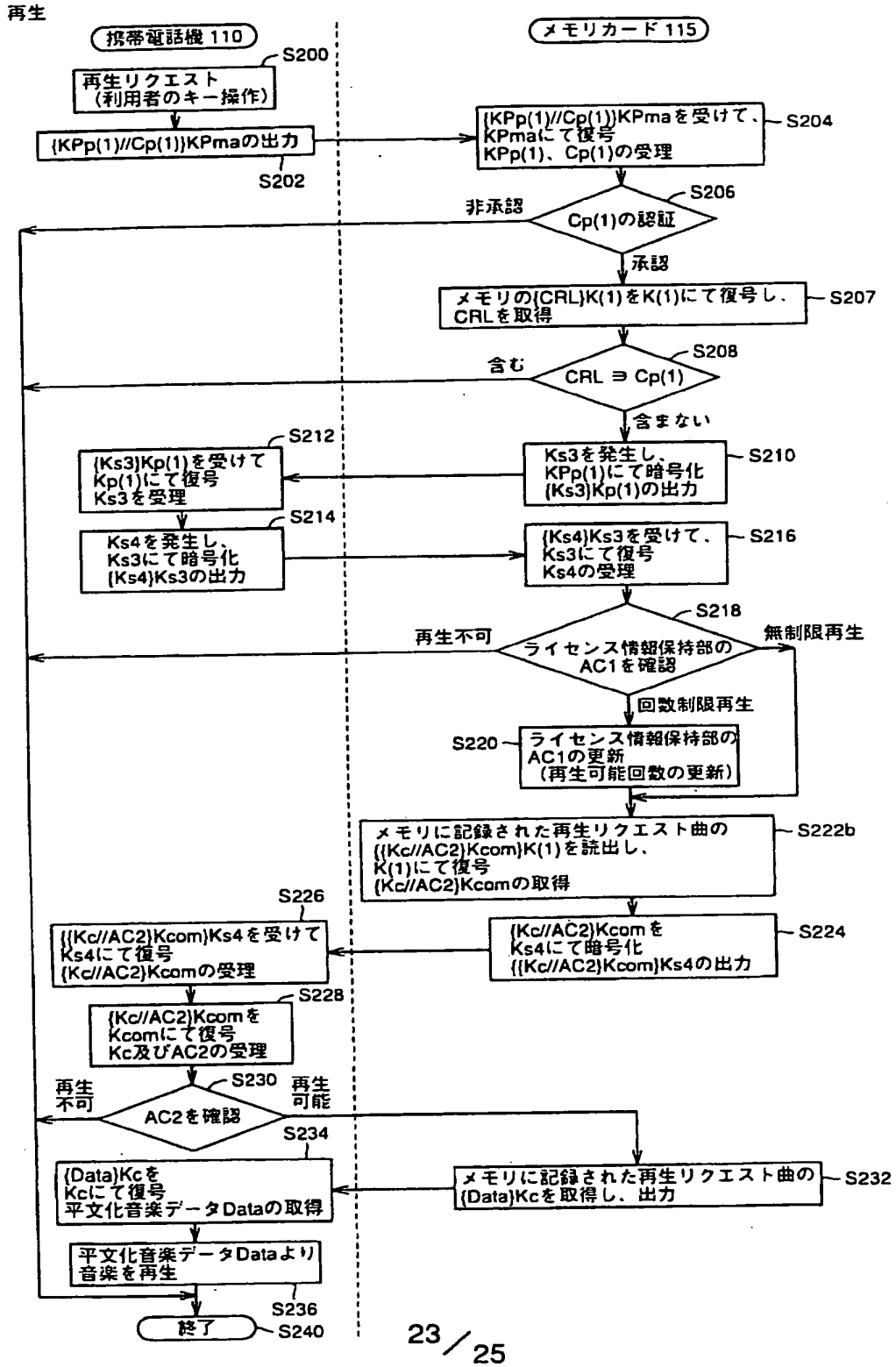

再生
携帯電話機 110
メモリカード 115
S200
再生リクエスト
(利用者のキー操作)
{KPp(1)//Cp(1)}KPmaの出力
S202
{KPp(1)//Cp(1)}KPmaを受けて、
KPmaにて復号
KPp(1)、Cp(1)の受理
S204
S206
非承認
Cp(1)の認証
承認
メモリの{CRL}K(1)をK(1)にて復号し、
CRLを取得
S207
S208
含む
CRL ∋ Cp(1)
含まない
S212
{Ks3}Kp(1)を受けて
Kp(1)にて復号
Ks3を受理
Ks3を発生し、
KPp(1)にて暗号化
{Ks3}Kp(1)の出力
S210
S214
Ks4を発生し、
Ks3にて暗号化
{Ks4}Ks3の出力
{Ks4}Ks3を受けて、
Ks3にて復号
Ks4の受理
S216
S218
再生不可
ライセンス情報保持部の
AC1を確認
無制限再生
回数制限再生
S220
ライセンス情報保持部の
AC1の更新
(再生可能回数の更新)
メモリに記録された再生リクエスト曲の
{{Kc//AC2}Kcom}K(1)を読出し、
K(1)にて復号
{Kc//AC2}Kcomの取得
S222b
S226
{{Kc//AC2}Kcom}Ks4を受けて
Ks4にて復号
{Kc//AC2}Kcomの受理
{Kc//AC2}Kcomを
Ks4にて暗号化
{{Kc//AC2}Kcom}Ks4の出力
S224
S228
{Kc//AC2}Kcomを
Kcomにて復号
Kc及びAC2の受理
再生
不可
S230
AC2を確認
再生
可能
S234
{Data}Kcを
Kcにて復号
平文化音楽データDataの取得
メモリに記録された再生リクエスト曲の
{Data}Kcを取得し、出力
S232
平文化音楽データDataより
音楽を再生
S236
終了
S240

FIG.24

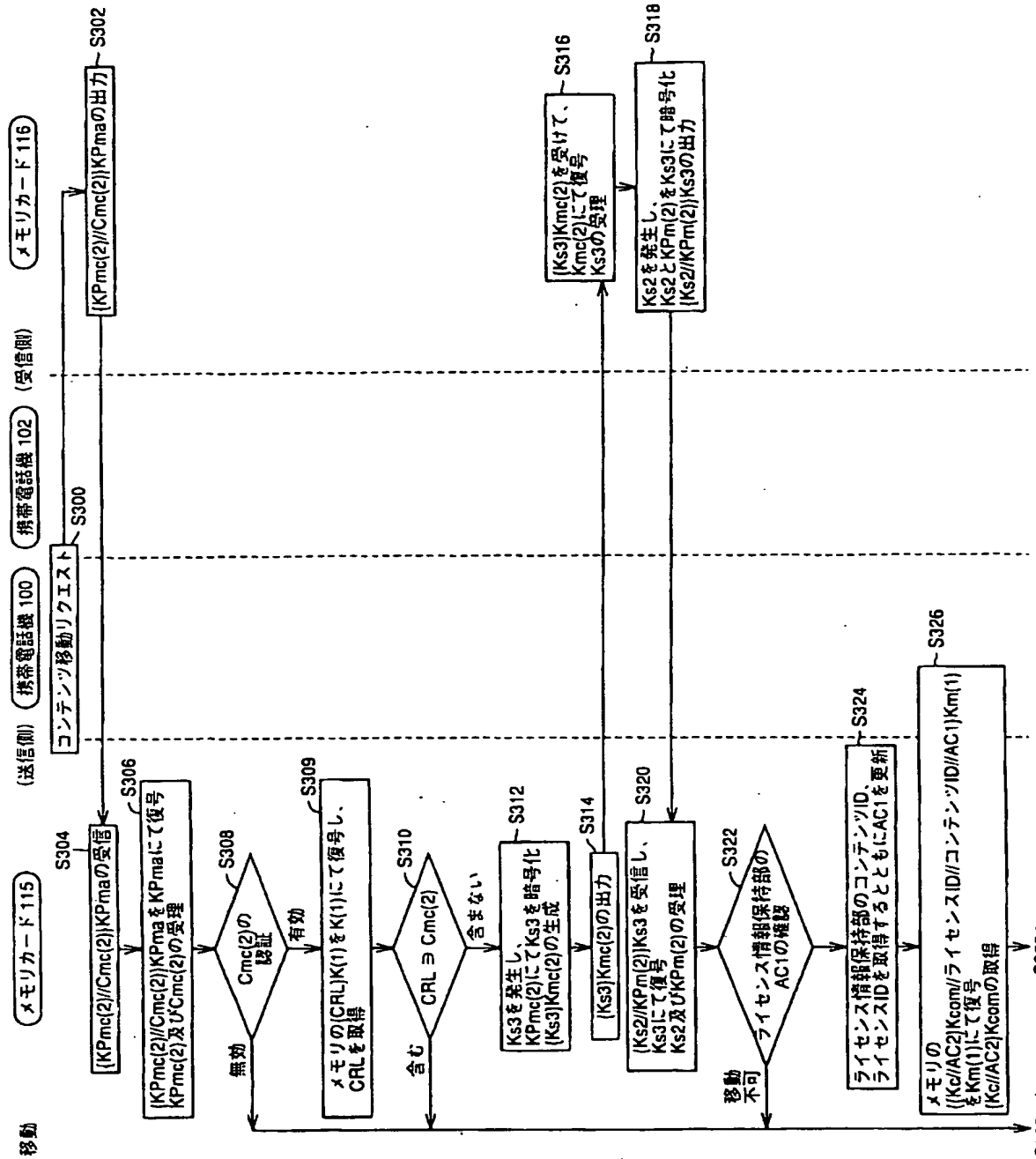
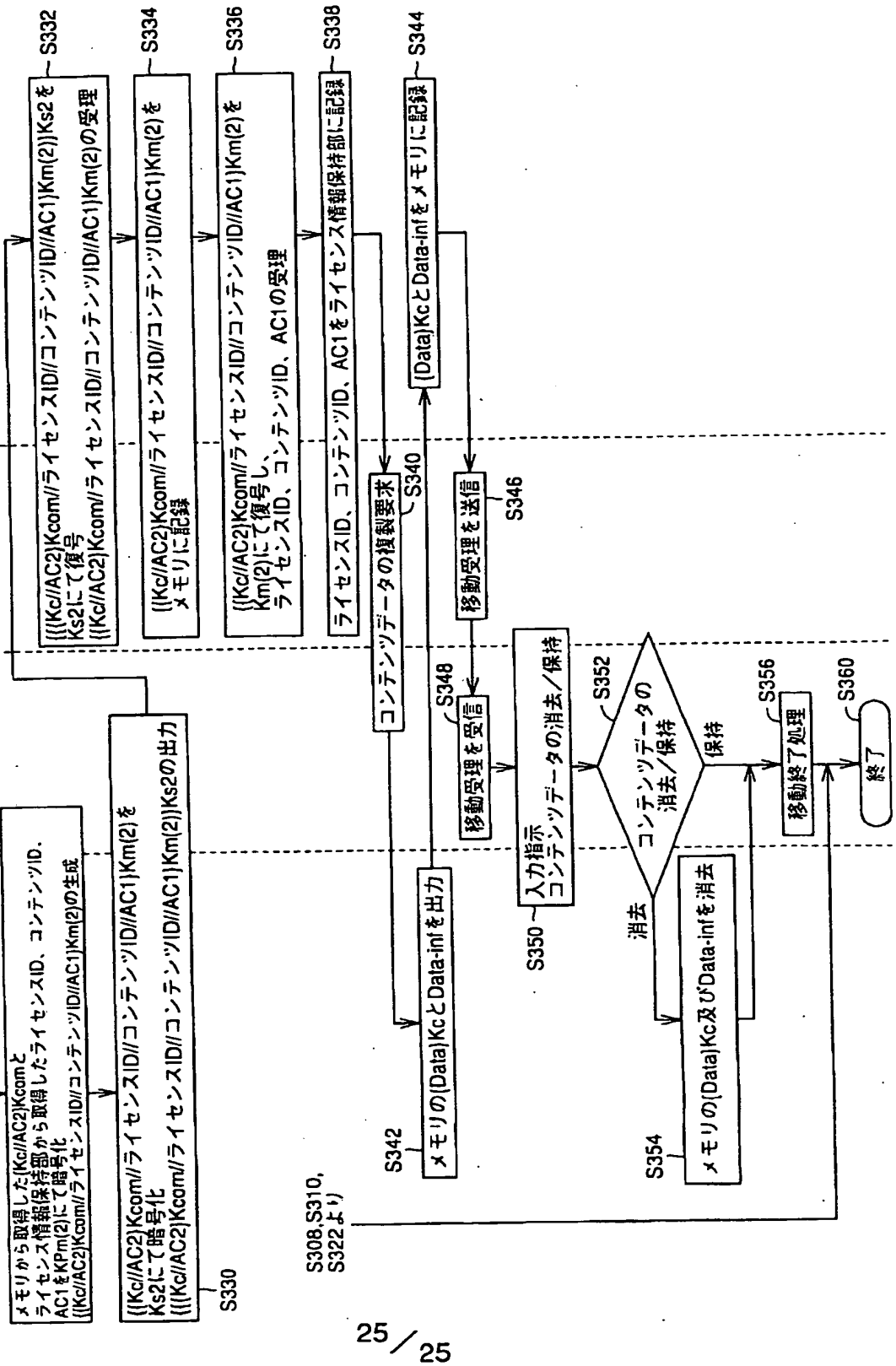

移動
メモリカード115
(送信側)
携帯電話機100
携帯電話機102
(受信側)
メモリカード116
コンテンツ移動リクエスト
S300
[KPmc(2)//Cmc(2)]KPmaの出力
S302
[KPmc(2)//Cmc(2)]KPmaの受信
S304
[KPmc(2)//Cmc(2)]KPmaをKPmaにて復号
KPmc(2)及びCmc(2)の受理
S306
Cmc(2)の認証
S308
無効
有効
メモリの(CRL)K(1)をK(1)にて復号し、
CRLを取得
S309
CRL ∋ Cmc(2)
S310
含む
含まない
Ks3を発生し、
KPmc(2)にてKs3を暗号化
[Ks3]Kmc(2)の生成
S312
[Ks3]Kmc(2)の出力
S314
[Ks3]Kmc(2)を受けて、
Kmc(2)にて復号
Ks3の受理
S316
[Ks2//KPm(2)]Ks3を受信し、
Ks3にて復号
Ks2及びKPm(2)の受理
S320
Ks2を発生し、
Ks2とKPm(2)をKs3にて暗号化
[Ks2//KPm(2)]Ks3の出力
S318
ライセンス情報保持部のAC1の検証
S322
移動不可
ライセンス情報保持部のコンテンツID、
ライセンスIDを取得するとともにAC1を更新
S324
メモリの
[(Kc//AC2]Kcom//ライセンスID//コンテンツID//AC1)Km(1)
をKm(1)にて復号
[Kc//AC2]Kcomの取得
S326
S328へ
S360へ

FIG.25


メモリカード110
携帯電話機100
携帯電話機102
メモリカード112
S326より
S328
メモリから取得した{Kc//AC2}Kcomと
ライセンス情報保持部から取得したライセンスID、コンテンツID、
AC1をKPm(2)にて暗号化
{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(2)の生成
{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(2)を
Ks2にて暗号化
{{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(2)}Ks2の出力
S330
{{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(2)}Ks2を
Ks2にて復号
{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(2)の受理
S332
{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(2)を
メモリに記録
S334
{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(2)を
Km(2)にて復号し、
ライセンスID、コンテンツID、AC1の受理
S336
ライセンスID、コンテンツID、AC1をライセンス情報保持部に記録
S338
コンテンツデータの複製要求
S340
{Data}KcとData-infをメモリに記録
S344
移動受理を送信
S346
移動受理を受信
S348
入力指示
コンテンツデータの消去／保持
S350
S352
コンテンツデータの
消去／保持
消去
保持
S354
メモリの{Data}Kc及びData-infを消去
S356
移動終了処理
S360
終了
S342
メモリの{Data}KcとData-infを出力
S308,S310,
S322より

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/08497

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L 9/32 G06F 12/14, 320 G10K 15/02 G06F 13/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L 9/00 H04K 1/00-3/00 G09C 1/00-5/00
G06F 12/00-13/00 G10K 15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST FILE(JOIS)
WPI(DIALOG)
INSPEC(DIALOG)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Digital Transmission Content Protection Specification, Volume 1 (Informational Version), Revision 1.0, (1999 April)	1-39
EA	JP, 2000-357127, A (Toshiba Corporation), 26 December, 2000 (26.12.00) (Family: none)	1-39
A	JP, 6-326786, A (Hitachi Denshi, Ltd.), 25 November, 1994 (25.11.94) (Family: none)	1-39
A	JP, 11-328850, A (Sony Corporation), 30 November, 1999 (30.11.99) & WO, 99/59092, A1 & EP, 996074, A	1-39

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
08 March, 2001 (08.03.01)	21 March, 2001 (21.03.01)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

国際調査報告

国際出願番号 PCT／JP00／08497

A. 発明の属する分野の分類（国際特許分類（IPC））
Int. Cl'
H04L 9／32 G06F 12／14, 320 G10K 15／02 G06F 13／00

B. 調査を行った分野
調査を行った最小限資料（国際特許分類（IPC））
Int. Cl'
H04L 9／00 H04K 1／00－3／00 G09C 1／00－5／00
G06F 12／00－13／00 G10K 15／00

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報 1922－1996年
日本国公開実用新案公報 1971－2001年
日本国登録実用新案公報 1994－2001年
日本国実用新案登録公報 1996－2001年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）
JICSTファイル（JOIS）
WPI（DIALOG）
INSPEC（DIALOG）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	Digital Transmission Content Protection Specification, Volume 1 (Informational Version), Revision 1.0, (1999 April)	1-39
EA	JP, 2000－357127, A（株式会社東芝）26. 12月. 2000（26. 12. 00）, ファミリーなし	1-39

☑ C欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 08. 03. 01

国際調査報告の発送日 21.03.01

国際調査機関の名称及びあて先
日本国特許庁（ISA／JP）
郵便番号100－8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員） 5W 9570
丸山 高政

電話番号 03－3581－1101 内線 3574

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ００／０８４９７

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ａ	ＪＰ，６－３２６７８６，Ａ（日立電子株式会社） ２５．１１月．１９９４（２５．１１．９４）， ファミリーなし	1-39
Ａ	ＪＰ，１１－３２８８５０，Ａ（ソニー株式会社） ３０．１１月．１９９９（３０．１１．９９）， ＆　ＷＯ，９９／５９０９２，Ａ１　＆　ＥＰ，９９６０７４，Ａ	1-39